The generalized Riemann hypothesis for Dirichlet L-functions

27 November 2026 · Edition 930

Volume V

Class groups, special values and strict orders

Abstract

We express strict orders in terms of Kummer classes, special values and norm maps. We use a single determinant to measure full strict orders at several twists, including classes that capitulate. For an extension ramified at two primes we prove that one decomposition group can detect every strict class. This gives full vanishing for specified character components across all twists with trivial residual character.

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

Contents

V Class groups, special values and strict orders 1
24 Kummer classes and real class groups . . . 3
24.1 Strict classes as triangular extensions . . . 3
24.2 A class-group test for the complementary sign . . . 4
24.3 Reflection without a local residual hypothesis . . . 6
24.4 Primes dividing the character order . . . 8
24.4.1 Descent to the fixed prime-power subfield . . . 8
24.5 Finite coefficients and Kummer classes on the first cyclotomic layer . . . 11
24.5.1 A description independent of the integral twist . . . 11
24.5.2 The ideal class and the local generators . . . 12
24.5.3 A test for every twist on the full family . . . 12
24.6 Large coefficient primes and totally real class groups . . . 14
24.7 A finite class group test at the coefficient prime . . . 16
24.8 Vanishing for cubic residual characters . . . 18
24.9 Vanishing on the real quartic field of conductor sixteen . . . 20
24.10 Locally trivial twists on the full real cyclotomic tower . . . 22
25 Special values and integral annihilators . . . 24
25.1 Strict classes and finite even K-groups . . . 24
25.2 Special values and the two conjugation eigenspaces . . . 26
25.3 Bernoulli sums for characters at every two-power layer . . . 28
25.4 An integral annihilator across the twists . . . 30
25.5 An annihilator at primes dividing the field degree . . . 32
25.6 Bernoulli units at large two-power conductor . . . 35
25.7 Effective descent in the real cyclotomic tower . . . 37
25.8 Bernoulli values shared by different coefficient primes . . . 39
25.9 Character comparison at primes dividing the degree . . . 42
25.10 Omitted Euler factors at the nonpositive integers . . . 45
26 Norms and cyclic character fields . . . 46
26.1 Norms of ideal classes and the exponents of strict classes . . . 46
26.1.1 An exact nonzero component in every matching twist . . . 48

26.2 A single relative class group for all twists at a prime . . . 49
26.3 Real cyclic quartic and sextic fields . . . 51
26.4 Norms of ideal classes in the remaining cohomology estimate . . . 56
26.5 A bound for all twists from two fields at each prime . . . 57
26.6 Vanishing at quartic and sextic residual characters . . . 58
26.7 A bound in every twist on a cyclic sextic subfield . . . 59
26.8 The full strict groups over the cyclic sextic field . . . 60
26.9 Two infinite families of character fields with exact strict orders . . . 61
26.10 Exact strict groups for cyclic fields with several ramified primes . . . 62
26.11 Tame inertia and the strict group in every dyadic layer . . . 65
26.12 Cyclic descent at every precision and the split coefficient prime . . . 67
26.13 Tame ramification in the moving quadratic components . . . 69
26.14 All weights on a family of cyclic sextic character fields . . . 72
27 Cyclotomic indices at finite primes . . . 74
27.1 Cyclotomic indices and strict orders . . . 74
27.2 The distribution of the cyclotomic valuations . . . 76
27.3 The cyclotomic index at an arbitrary odd prime . . . 77
27.4 Cyclotomic classes that reduce to rational Kummer classes . . . 78
27.5 A vanishing result for fields ramified at one prime . . . 79
27.6 Two Frobenius evaluations at conductor 1799 . . . 80
27.7 Class groups and strict classes throughout one cyclotomic extension . . . 81
27.8 An exact strict order at conductor 257 . . . 82
27.9 Class numbers in every layer of the cyclotomic tower at three . . . 83
28 Positive twists and explicit strict orders . . . 84
28.1 Local conditions for the positive cyclotomic twist . . . 84
28.2 Primitive special values for the positive twist . . . 85
28.3 Every strict twist at eleven in the conductor forty-one tower . . . 86
28.4 Testing the order of a strict group at finite level . . . 88
28.5 A local correction of unbounded length at 37 . . . 89
28.6 Positive twists with a ramified or exceptional local character . . . 90
28.7 Two residue computations at eleven for conductor forty-one . . . 91
28.8 The local correction to the interpolated order . . . 92
28.9 Removing the factor forced by local torsion . . . 93
28.10 A split uniformizer test for strict quadratic classes . . . 95
28.11 Local cyclotomic degrees and ordinary class groups . . . 96
28.12 An exact split contribution of order nine . . . 97
28.13 Characteristic polynomials and capitulation in the real tower . . . 98
28.14 A determinant for full strict orders and the first class norm . . . 100
28.15 A decomposition group that detects every strict class . . . 102
29 References . . . 106

24 Kummer classes and real class groups

24.1 Strict classes as triangular extensions

We describe the arithmetic group whose length would have to be compared with (30.6). Let $E/\mathbb{Q}$ be finite abelian with group G, let $\ell \nmid |G|$ be odd, and choose the valuation ring $\mathcal{O}$ of a finite unramified extension $J/\mathbb{Q}_\ell$ containing all values of the characters of G. Such a ring exists because $|G|$ is prime to ℓ. For a character $\alpha : G \to \mathcal{O}^\times$ put

$$e_\alpha = |G|^{-1} \sum_{g \in G} \alpha(g)^{-1} g, \qquad \vartheta = \kappa_\ell^{-r} \alpha^{-1}, \qquad D = (J/\mathcal{O})(\vartheta).$$

Here the character of G is inflated to the absolute Galois group $G_\mathbb{Q}$. Define a strict group over $\mathbb{Q}$ as the subgroup of $H^1(G_\mathbb{Q}, D)$ of classes trivial on inertia at every $p \neq \ell$ and trivial on the full decomposition group at ℓ.

Theorem 24.1 (Character descent)**.** *There is an isomorphism of $\mathcal{O}$-modules between this strict group and $e_\alpha(\mathcal{S}_{\ell,r}(E) \otimes_{\mathbb{Z}_\ell} \mathcal{O})$. The $\mathcal{S}_{\ell,r}(E)$ in this formula has the same unramified and strict local conditions as in Volume II. For $E = E_x$ the theorem applies to every odd $\ell \nmid \operatorname{ord}(\psi)$. The component with $\alpha(c) = (-1)^r$ corresponds exactly to an even character ϑ.*

Proof. On G_E the finite character α is trivial. Restriction on absolute cohomology identifies $H^1(G_\mathbb{Q}, D)$ with $H^1(G_E, D)^G$, by inflation–restriction: the outside terms in degrees one and two for the finite quotient acting on D^{G_E} vanish by averaging. Restricting coefficients to G_E and then twisting the G-action back by α^{-1} identifies this invariant subspace with the displayed idempotent on unrestricted cohomology of E. Tensoring by $\mathcal{O}$ commutes with continuous cohomology here, as $\mathcal{O}$ is finite free over $\mathbb{Z}_\ell$. Inflation from G_{E,S_ℓ} identifies unramified classes outside ℓ with the classes having trivial inertia there, since the coefficient is unramified away from ℓ over E.

For inertia over $p \neq \ell$, the quotient of the inertia group over $\mathbb{Q}$ by inertia over E has order dividing $|G|$. Inflation–restriction therefore gives injectivity on local H^1 upon restriction, including when α is ramified. The same holds for full decomposition groups over ℓ. The local conditions descend in both directions. Finally $[E_x : \mathbb{Q}] \mid 4\,2^l \operatorname{ord}(\psi)$, and $\vartheta(c) = (-1)^r \alpha(c)^{-1}$. This proves all assertions. □

Under this description a class is represented by a continuous function $z : G_\mathbb{Q} \to J/\mathcal{O}$ satisfying

$$z(gh) = z(g) + \vartheta(g) z(h).$$

Equivalently, it gives affine transformations $y \mapsto \vartheta(g) y + z(g)$. Changing the origin adds a coboundary to z. The strict local condition means that an origin can be chosen locally so that the translations disappear on the required local group. A continuous cocycle has finite image by compactness, hence takes values in $\ell^{-m}\mathcal{O}/\mathcal{O}$ for some m. After multiplication by ℓ^m in representatives, identify this module with $\mathcal{O}/\ell^m\mathcal{O}$ and write $\bar z$ for its coordinate. The finite-level extensions have the matrices

$$g \longmapsto \begin{pmatrix} \vartheta(g) & \bar z(g) & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \vartheta(g)^{-1} \end{pmatrix} \pmod{\ell^m}.$$

Their multiplication law is precisely the cocycle law. Their trace is $\vartheta(g) + 1 + \vartheta(g)^{-1}$ for every z. At a good arithmetic Frobenius at p, this is the reduction of d_α. Thus the upper-right entry carries extension information that these traces alone do not detect. For instance the nonzero

homomorphism from the cyclic group of order ℓ to the additive group of $\mathbf{F}_\ell$ gives a nonsplit unipotent extension with the trace of the split extension at every element.

To deduce a bound for the strict groups from (30.6), the proposed argument needs an integral deformation theorem that bounds their lengths using congruences with the characteristic-zero systems counted above. It also needs level and weight control for the systems that theorem produces. In the source archive, `UnitaryThreeGroups/OneCharOf.lean` in the automorphic varieties directory, lines 102–138, uses a deformation ring, its integral model and automorphy of its points in deriving the single-character length inequality. Formula (30.5) proves the congruence-ideal calculation for the Hecke traces. Theorem 24.1 identifies the strict classes on the other side. A comparison of these two integral modules, with uniform length bounds, has not been established here.

24.2 A class-group test for the complementary sign

Retain $E = E_x \subseteq \mathbb{Q}(\zeta_N)$, $\alpha, \mathcal{O}, J, \vartheta, D$ from Theorem 24.1. Suppose ℓ is odd, $\ell \nmid [E:\mathbb{Q}]$, $\alpha(c) = (-1)^r$, and the reduction $\bar{\vartheta}$ is nontrivial on $G_{\mathbb{Q}_\ell}$. The last condition is automatic if $\ell \nmid N$ and $\ell - 1 \nmid r$: at such a prime α is unramified and the mod-ℓ cyclotomic character maps inertia onto $\mathbf{F}_\ell^\times$. Denote the strict group over $\mathbb{Q}$ in Theorem 24.1 by S_α. For $m \geq 1$ put

$$n_m = N\ell^m, \quad L_m = \mathbb{Q}(\zeta_{n_m}), \quad \Gamma_m = \mathrm{Gal}(L_m/\mathbb{Q}), \quad R_m = \mathcal{O}/\ell^m\mathcal{O}, \qquad \beta_m = \kappa_{\ell,m}^{r+1}\alpha \bmod \ell^m.$$

Here $\kappa_{\ell,m}$ is the cyclotomic character modulo ℓ^m. For an $R_m[\Gamma_m]$-module U, let $U[\beta_m]$ be the subgroup on which every γ acts as $\beta_m(\gamma)$. This definition also applies when $\ell \mid |\Gamma_m|$.

Theorem 24.2 (Reflection at every exponent)**.** *After choosing a generator of μ_{ℓ^m}, there is an R_m-linear injection*

$$S_\alpha[\ell^m] \;\hookrightarrow\; \big(\mathrm{Cl}(\mathcal{O}_{L_m})[\ell^m] \otimes_{\mathbb{Z}_\ell} \mathcal{O}\big)[\beta_m]. \tag{24.1}$$

In particular the target lies in the minus part of the ideal class group.

Proof. Consider $0 \to D[\ell^m] \to D \xrightarrow{\ell^m} D \to 0$. On a group U the kernel on H^1 from finite to divisible coefficients is $D^U/\ell^m D^U$. At $U = G_\mathbb{Q}$ and $U = G_{\mathbb{Q}_\ell}$ the invariants vanish: an element with $\bar{\vartheta} \neq 1$ acts by a scalar whose difference from one is a unit in $\mathcal{O}$. At inertia over $p \neq \ell$, the cyclotomic character is unramified and the inertia action through α has order prime to ℓ. If it is nontrivial its invariants vanish by the same argument. Otherwise $D^U = D$ is divisible. In every case the finite-coefficient map is locally injective. Exactness globally now identifies $S_\alpha[\ell^m]$ with the classes for $R_m(\vartheta)$ which are unramified away from ℓ and zero on the full decomposition group at ℓ.

The coefficient is trivial over L_m. Restriction from $G_\mathbb{Q}$ to G_{L_m} on these degree-one classes is injective even when $\ell \mid |\Gamma_m|$. Its kernel inflates from $H^1(\Gamma_m, R_m(\vartheta))$. Choose $\tau \in \Gamma_m$ with $\vartheta(\tau) - 1$ a unit. For a cocycle z on the abelian group Γ_m, evaluate $z(\tau\sigma) = z(\sigma\tau)$. The identity

$$(\vartheta(\tau) - 1)z(\sigma) = (\vartheta(\sigma) - 1)z(\tau)$$

makes z the coboundary of $z(\tau)/(\vartheta(\tau) - 1)$. This proves injectivity.

Use the chosen root of unity to identify the trivial coefficient on G_{L_m} with $\mu_{\ell^m} \otimes_{\mathbb{Z}/\ell^m} R_m$. Under this change the action on the restricted classes is by $\beta_m = \kappa_{\ell,m}\vartheta^{-1}$. Indeed a restricted cocycle is a homomorphism b satisfying $b(\sigma h \sigma^{-1}) = \vartheta(\sigma) b(h)$. After identifying its values with roots of unity, conjugation on the values supplies the factor $\kappa_{\ell,m}(\sigma)$; precomposition with $h \mapsto \sigma^{-1} h \sigma$ supplies $\vartheta(\sigma)^{-1}$. Kummer theory thus gives classes in $(L_m^\times / L_m^{\times \ell^m}) \otimes R_m$ with this eigencharacter. Here tensoring over $\mathbb{Z}/\ell^m$ is exact since R_m is finite free over that ring.

For these classes every finite valuation is a multiple of ℓ^m, coordinate by coordinate in a basis of R_m. At places above ℓ, the local Kummer class is trivial. At the other places it becomes trivial over the maximal unramified extension, which has the same value group as the original local field. Taking the valuation of an ℓ^m-th root there proves the assertion. If $(a) = \mathfrak{a}^{\ell^m}$, send its Kummer class to $[\mathfrak{a}]$. The ambiguity of multiplying a by an ℓ^m-th power changes $\mathfrak{a}$ by a principal ideal. The resulting equivariant map to $\mathrm{Cl}(\mathcal{O}_{L_m})[\ell^m]$ has kernel the global units modulo ℓ^m-th powers: if $\mathfrak{a} = (b)$, a/b^{ℓ^m} is a unit. The same descriptions hold after tensoring.

The character β_m is odd because ϑ is even. The odd part of the unit quotient is generated by roots of unity. In fact $u/\bar{u}$ for any global unit has modulus one at every embedding and is an algebraic integer, hence is a root of unity by Kronecker's theorem. Since two is invertible, the differences $1 - c$ generate the odd part. On its root-of-unity generators the Galois action is $\kappa_{\ell,m}$; prime-to-ℓ torsion makes no contribution to this quotient. The character β_m differs from $\kappa_{\ell,m}$ on the residue field by our choice of τ, so an element with both actions is zero. This proves injectivity in (24.1). □

Theorem 24.3 (An explicit annihilator)**.** *For any positive integer b prime to $N\ell$ define*

$$A_{b,m}(\alpha, r) = \sum_{\substack{1 \le j \le n_m \\ (j, n_m) = 1}} \left\lfloor \frac{bj}{n_m} \right\rfloor \left(j^{r+1} \alpha(j) \right)^{-1} \quad \text{in } R_m. \tag{24.2}$$

This scalar kills $S_\alpha[\ell^m]$. If it is nonzero and its valuation is $v < m$, the entire finite group S_α is killed by ℓ^v. In particular any nonzero residue at $m = 1$ proves $S_\alpha = 0$ at every exponent. The scalars in (24.2) are compatible under reduction as m increases.

Proof. Write $\sigma_j(\zeta_{n_m}) = \zeta_{n_m}^{j}$ and let

$$\Theta_n = \frac{1}{n} \sum_{1 \le j \le n,\ (j,n)=1} j\, \sigma_j^{-1}, \qquad n = n_m.$$

The classical Stickelberger theorem states that the integral group-ring elements in $\mathbb{Z}[\Gamma_m]\Theta_n$ annihilate the ideal class group of the full cyclotomic field. Apply it to $(b - \sigma_b)\Theta_n$. The coefficient of σ_j^{-1} here is $bj/n - \{bj/n\} = \lfloor bj/n \rfloor$. Thus the element is integral. On the β_m-eigensubgroup in (24.1) its action is multiplication by (24.2). This proves the first assertion. [1]

If the scalar has valuation $v < m$, its unit factor is invertible in R_m. Hence $S_\alpha[\ell^m]$ is killed by ℓ^v. Any element of an ℓ-primary group of order higher than ℓ^v generates a cyclic subgroup containing an element of order exactly ℓ^{v+1}. That element already belongs to $S_\alpha[\ell^m]$, a contradiction. This proves the assertion about the full group.

To prove compatibility put $n = n_m$. Above each unit j mod n the units modulo $n\ell$ are $j + kn$, $0 \le k < \ell$, because $\ell \mid n$. Their coefficients in $\Theta_{n\ell}$ sum to $j/n + (\ell - 1)/2$. Thus projection to $\mathbb{Q}[\Gamma_m]$ takes $\Theta_{n\ell}$ to $\Theta_n + (\ell - 1)\sum_{g \in \Gamma_m} g/2$. Multiplication by $b - \sigma_b$ changes the difference into an integral multiple of $\sum_g g$. Its value on β_m is zero, since g and cg have opposite values and $\beta_m(c) = -1$. The character β_{m+1} reduces to β_m, giving the claimed compatibility. □

Corollary 24.4 (Application on the interval)**.** *For every x on the common intervals, every odd $\ell \nmid N \operatorname{ord}(\psi)$, and $1 \le r < t(x)$ with $\ell - 1 \nmid r$, Theorem 24.3 applies to each component of the sign $(-1)^r$ of the full group $\mathcal{S}_{\ell,r}(E_x)$. It tests every twist in the sum if $\ell > t(x) + 1$. More explicitly, a nonzero test of valuation v bounds the corresponding length by*

$$\operatorname{length}_{\mathcal{O}} S_\alpha \ \le\ v \, \dim_{\mathcal{O}/\ell}\big((\,\mathrm{Cl}(\mathcal{O}_{L_1})[\ell] \otimes_{\mathbf{F}_\ell} (\mathcal{O}/\ell)\big)[\beta_1]\big)\,.$$

Proof. The prime and twist conditions ensure nontrivial residual inertia at ℓ, as noted above. By Theorem 24.1 the complementary sign is the direct sum of these components after extending to $\mathcal{O}$. Extension of scalars from $\mathbb{Z}_\ell$ to the unramified $\mathcal{O}$ preserves length in their respective normalized units, by the structure theorem for finite modules. The number of cyclic summands of S_α is $\dim_{\mathcal{O}/\ell} S_\alpha[\ell]$, bounded by Theorem 24.2 with $m = 1$. Each summand has length at most v. □

For example, take $E = \mathbb{Q}(i)$, $N = 4$, $\ell = 3$, and odd r. The complementary character is the quadratic character α modulo four. At $m = 1$ the units modulo twelve are $1, 5, 7, 11$; their values under β_1 are $1, 1, -1, -1$, since $r + 1$ is even. With $b = 5$ the four floors are $0, 2, 2, 4$, giving $A_{5,1} = -4 \equiv 2 \bmod 3$. Thus the complementary group vanishes at three for every such twist. This example illustrates a local test. In the fields E_x of the prime count the residue sums vary with N, ℓ, α, r. Section 24.3 treats the other local types when the coefficient prime is prime to the field degree. The lengths for vanishing residues still require control. The divisibility theorem for Hecke congruences in Section 30.5 and the independent tests here leave this uniform arithmetic estimate outstanding.

24.3 Reflection without a local residual hypothesis

Let $E/\mathbb{Q}$ be abelian and let $\ell \nmid [E : \mathbb{Q}]$ be odd. Use $\alpha, \vartheta, D, S_\alpha$ as in Theorem 24.1, with $\alpha(c) = (-1)^r$. Let $k = \mathcal{O}/\ell\mathcal{O}$, write a bar for reduction to k, and put $f = \operatorname{cond}(\alpha)$ and $f' = f/\ell^{v_\ell(f)}$. Since the order of α is prime to ℓ, its local character at ℓ kills the principal units, a pro-ℓ group. Thus $v_\ell(f) \le 1$. For each $m \ge 1$ define

$$n = f'\ell^m, \qquad K_m = \mathbb{Q}(\zeta_n), \qquad R_m = \mathcal{O}/\ell^m\mathcal{O}, \qquad \beta_m = \kappa_{\ell,m}\,(\vartheta \bmod \ell^m)^{-1}.$$

Both α and $\kappa_{\ell,m}$ factor through $\operatorname{Gal}(K_m/\mathbb{Q})$. Using this field allows the reflection test to discard auxiliary conductor factors belonging to other characters.

Lemma 24.5 (Local valuation of a finite lift)**.** *Let F be a finite extension of $\mathbb{Q}_\ell$ containing μ_{ℓ^m}, and fix a generator identifying $\mathbb{Z}/\ell^m$ with μ_{ℓ^m}. If a continuous homomorphism $G_F \to \mathbb{Z}/\ell^m$ factors through $\operatorname{Gal}(F(\mu_{\ell^\infty})/F)$, its Kummer class is represented by a unit of F.*

Proof. The cyclotomic image of G_F is open in $1 + \ell^m\mathbb{Z}_\ell$. The ℓ-adic logarithm identifies this last group with $\ell^m\mathbb{Z}_\ell$, so the image is precisely $1 + \ell^a\mathbb{Z}_\ell$ for some $a \ge m$. A primitive ℓ^a-th root u then belongs to F. Choose v with $v^{\ell^m} = u$ and of order ℓ^{a+m}. The Kummer homomorphism of u is $g \mapsto g(v)/v = v^{\kappa_\ell(g)-1}$. It sends an element with cyclotomic value $1 + \ell^a$ to a primitive ℓ^m-th root of unity. That element generates the cyclotomic image topologically, as its logarithm has valuation a. Every homomorphism from this image to μ_{ℓ^m} is a multiple of the one for u. All its Kummer classes are consequently represented by powers of the unit u. After choosing a $\mathbb{Z}/\ell^m$-basis the same result applies to each coordinate for coefficients R_m. □

Theorem 24.6 (All complementary characters of prime-to-ℓ order)**.** *If $\bar\vartheta$ is trivial on $G_\mathbb{Q}$, then $S_\alpha = 0$. For every other $\bar\vartheta$ and every $m \ge 1$, a choice of ℓ^m-th root of unity of exact order ℓ^m gives an injection*

$$S_\alpha[\ell^m] \;\hookrightarrow\; (\operatorname{Cl}(\mathcal{O}_{K_m})[\ell^m] \otimes_{\mathbb{Z}_\ell} \mathcal{O})[\beta_m]. \tag{24.3}$$

This includes characters that become trivial modulo ℓ on the entire decomposition group at ℓ.

Proof. First suppose $\bar\vartheta = 1$ globally. Let ω be the Teichmüller lift of the mod-ℓ cyclotomic character. Reduction is injective on roots of unity of order prime to ℓ in $\mathcal{O}$. Thus $\alpha = \omega^{-r}$ and $\vartheta = (\kappa_\ell/\omega)^{-r}$. It is unramified at every finite prime other than ℓ. Let $G_{\mathbb{Q},S_\ell}$ allow ramification

at ℓ and the infinite place. Every class in S_α inflates from this quotient. Indeed, the inertia groups away from ℓ act trivially on D, so restriction to each of them is an actual homomorphism. The class condition makes it zero on those groups and hence on their closed normal closure.

We show that $H^1(G_{\mathbb{Q},S_\ell}, D)[\ell] = 0$. The group $D[\ell]$ has trivial action and identifies with the additive group of k. Every continuous homomorphism $G_{\mathbb{Q},S_\ell} \to k$ factors through the pro-ℓ part of $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q})$, which is $1+\ell\mathbb{Z}_\ell$. This follows from Kronecker–Weber. In a finite cyclotomic field of modulus $d\ell^a$, $(d,\ell) = 1$, the factors at primes dividing d are generated by their inertia groups, using total ramification in each prime-power cyclotomic field and unramifiedness of the other factors at that prime. The characters here kill all such inertia and the prime-to-ℓ part of $\mathbb{Z}_\ell^\times$. The space of homomorphisms is therefore one-dimensional over k, by the logarithm on principal units. [2]

Set $s = 1 + v_\ell(r)$ and take $z = \ell^{-(s+1)} + \mathcal{O} \in J/\mathcal{O}$. The coboundary $g \mapsto (\vartheta(g) - 1)z$ has values in $D[\ell]$. All values $\vartheta(g) - 1$ belong to $\ell^s\mathbb{Z}_\ell$, and some have valuation exactly s, by taking $\kappa_\ell(g) = 1+\ell$. Indeed multiplication by $-r$ on logarithms takes $\ell\mathbb{Z}_\ell$ onto $\ell^s\mathbb{Z}_\ell$. This coboundary represents a nonzero generator of the finite-coefficient homomorphism space. Every k-multiple is also a coboundary with values in D, by lifting the scalar to $\mathcal{O}$. The coefficient sequence for multiplication by ℓ now shows the asserted vanishing of $H^1(G_{\mathbb{Q},S_\ell}, D)[\ell]$. Every continuous cocycle with values in the discrete ℓ-primary group D has finite image, hence is killed by some power of ℓ. A nonzero such cohomology group would have an element of order ℓ. This proves the first case.

Now assume $\bar\vartheta \neq 1$ globally. There is $\tau \in G_\mathbb{Q}$ such that $\vartheta(\tau) - 1$ is a unit. In particular $D^{G_\mathbb{Q}} = 0$. Every class of $S_\alpha[\ell^m]$ has a unique finite-coefficient cohomology class above it by the coefficient exact sequence. Restriction of that class to K_m is injective: on the finite abelian group $\mathrm{Gal}(K_m/\mathbb{Q})$, the cocycle identity with τ in the proof of Theorem 24.2 makes every cocycle with these coefficients a coboundary. After choosing the root of unity, the restricted classes are Kummer classes of character β_m, as in that proof.

We check the valuation at every finite place. Away from ℓ, on inertia over K_m one has $\alpha = 1$ and $\kappa_\ell = 1$. A finite representative of a strict class therefore vanishes there: in divisible coefficients it equals a coboundary on the original inertia, and that coboundary restricts to zero. The local Kummer class becomes trivial over the maximal unramified extension. Its valuation is a multiple of ℓ^m because that extension has the same value group. At a place $w \mid \ell$ the divisible class is locally trivial. For its finite representative there is $z_w \in D$ with

$$b(g) = (\vartheta(g) - 1)z_w \qquad (g \in G_{K_{m,w}}).$$

Here $b(g) \in D[\ell^m]$, the finite coefficient action over $K_{m,w}$ is trivial, and $\alpha(g) = 1$. Thus the homomorphism b vanishes on the kernel of κ_ℓ. Lemma 24.5 shows that each coordinate of its local Kummer class is represented by a unit. This supplies the required valuation at w even if the finite class there is nonzero.

The ideal-class map in the proof of Theorem 24.2 therefore applies with K_m. Its kernel consists of unit classes. Its odd part is generated by roots of unity, with character $\kappa_{\ell,m}$, by the same argument with $u/\bar u$. On τ the difference between β_m and $\kappa_{\ell,m}$ is a unit because $\vartheta(\tau) - 1$ is a unit. The kernel consequently meets our β_m-classes only in zero. This proves (24.3). □

Corollary 24.7 (The finite test on the entire prime-to-degree range)**.** *On the fields E_x of Volume IV, for every odd $\ell \nmid \mathrm{ord}(\psi)$, every $1 \le r < \lfloor x^{401} \rfloor$ and every character of the complementary sign, the following alternatives give a test. If $\alpha = \omega^{-r}$ the component vanishes.*

Otherwise, for any $m \geq 1$ and any positive integer b coprime to $f'\ell$, the element

$$\sum_{\substack{1\leq j\leq f'\ell^m\\(j,f'\ell)=1}} \left\lfloor \frac{bj}{f'\ell^m} \right\rfloor (j^{r+1}\alpha(j))^{-1} \pmod{\ell^m} \tag{24.4}$$

annihilates $S_\alpha[\ell^m]$. A nonzero residue of valuation $v < m$ proves that $\ell^v S_\alpha = 0$. In particular a unit at the first level proves vanishing for every positive twist in the same class modulo $\ell - 1$ with this α.

Proof. The degree of E_x divides $4\cdot 2^l \operatorname{ord}(\psi)$. Apply Theorems 24.1 and 24.6. The computation of $(b-\sigma_b)\Theta_n$ and the cyclic-subgroup argument of Theorem 24.3 apply verbatim to the modulus $f'\ell^m$ and the target in (24.3). At $m = 1$ the powers j^{r+1} depend only on r mod $(\ell - 1)$; parity also stays fixed in that class. This gives the last assertion. □

For an example with locally trivial residual character take $E = \mathbb{Q}(i, \sqrt{13})$, $\ell = 3$, any positive even r, and the quadratic character α of conductor 13. The degree is four and $(3/13) = 1$, so $\bar{\vartheta}$ is trivial at three. Its restriction to inertia at thirteen is nontrivial. In (24.4) take $m = 1, b = 2$, hence $n = 39$. The floor is one on the twelve units between 20 and 38, and zero on the other units. On these twelve the inverse character modulo three has value $+1$ at $20, 22, 25, 32$ and value -1 at the other eight, by the squares $1, 3, 4, 9, 10, 12$ modulo thirteen. The sum is $-4 \equiv 2 \pmod 3$. The entire component vanishes for every such r.

For the sum of lengths in Volume I, a unit removes a component outright. Where the first residues vanish, the exponent requires bounds at higher levels, together with bounds for the numbers of cyclic summands. The test covers every twist at primes coprime to the field degree, including primes ramified in the conductor. Section 24.4 treats the primes dividing the character order.

24.4 Primes dividing the character order

We extend the class-group test to the primes dividing the degree of the full field. For this purpose we take the character components over an intermediate field of odd prime-power degree. A determinant over its Galois group will provide an annihilator even though its group order is zero modulo the coefficient prime.

24.4.1 Descent to the fixed prime-power subfield

Let $E/\mathbb{Q}$ be finite abelian, ℓ an odd prime, and write $G = \operatorname{Gal}(E/\mathbb{Q}) = P \times H$, where P is its ℓ-Sylow subgroup and H has order prime to ℓ. Let $K = E^H$, so $P = \operatorname{Gal}(K/\mathbb{Q})$, and write $d = [K : \mathbb{Q}]$. The field K is totally real since complex conjugation has order at most two. Take a finite unramified coefficient ring $\mathcal{O}$ over $\mathbb{Z}_\ell$ containing the values of all characters of H, with fraction field J. For $\alpha \in \widehat{H}$, let $\widetilde{\alpha}$ be its extension to G that is trivial on P. View it as a Dirichlet character, or equivalently as a character of $G_\mathbb{Q}$. Set $\vartheta = \kappa_\ell^{-r}\widetilde{\alpha}^{-1}$, $D = (J/\mathcal{O})(\vartheta)$, and use the complementary sign $\alpha(c) = (-1)^r$. Write $S_\alpha(K)$ for the classes in $H^1(K, D)$ trivial on inertia away from ℓ and trivial on all decomposition groups over ℓ.

Lemma 24.8. *With $e_\alpha = |H|^{-1}\sum_{h\in H}\alpha(h)^{-1}h$, restriction gives*

$$S_\alpha(K) \;\simeq\; e_\alpha(\mathcal{S}_{\ell,r}(E) \otimes_{\mathbb{Z}_\ell} \mathcal{O}).$$

For the fields E_x, the field K is the subfield of K_ψ of degree $\ell^{v_\ell(\operatorname{ord}(\psi))}$; in particular it is fixed as x, q, d vary.

Proof. Apply inflation–restriction to E/K. All higher cohomology of the finite quotient H on ℓ-primary modules vanishes by averaging. On G_E the finite character is trivial, and twisting the quotient action by α^{-1} selects exactly e_α. At every finite place the corresponding decomposition or inertia quotient has order dividing $|H|$; its first cohomology vanishes, so the restriction on the relevant local H^1 is injective. This proves the equality of local conditions just as in Theorem 24.1. For E_x/K_ψ the relative degree is a power of two. Restriction to K_ψ therefore identifies the ℓ-Sylow subgroups, and the indicated subfield of the cyclic extension $K_\psi/\mathbb{Q}$ has precisely that prime-power degree. □

For $m \geq 1$, let f_K be the conductor of the abelian extension $K/\mathbb{Q}$, let f_α be that of $\widetilde{\alpha}$, and put

$$n_m = \operatorname{lcm}(f_K, f_\alpha, \ell^m), \qquad L_m = \mathbb{Q}(\zeta_{n_m}),$$
$$G_m = \operatorname{Gal}(L_m/\mathbb{Q}), \qquad \Gamma_m = \operatorname{Gal}(L_m/K), \qquad R_m = \mathcal{O}/\ell^m\mathcal{O}.$$

Use $\widetilde{\beta}_m = \kappa_{\ell,m}^{r+1}\widetilde{\alpha} \bmod \ell^m$ on G_m, and write β_m for its restriction to Γ_m. For an element $\sigma \in G_m$ write $[\sigma|_K]$ for the basis vector in the group algebra $R_m[P]$.

Theorem 24.9 (A determinant annihilator)**.** *Suppose $\bar{\vartheta}$ is nontrivial on G_K. For every positive integer b prime to n_m, form the following element of the group algebra and determinant in R_m:*

$$U_{b,m} = \sum_{\substack{1\leq j\leq n_m\\(j,n_m)=1}} \left\lfloor \frac{bj}{n_m} \right\rfloor (j^{r+1}\widetilde{\alpha}(j))^{-1}[\sigma_j^{-1}|_K],$$
$$B_{b,m} = \det\left(u \mapsto U_{b,m}u \mid R_m[P]\right), \qquad \sigma_j(\zeta_{n_m}) = \zeta_{n_m}^{j}. \tag{24.5}$$

Then $B_{b,m}$ annihilates $S_\alpha(K)[\ell^m]$. If it has valuation $v < m$ it follows that $\ell^v S_\alpha(K) = 0$. For $m = 1$ the determinant is the d-th power of the sum of the coefficients of $U_{b,1}$. Thus one scalar sum modulo ℓ already suffices for the vanishing test, including when $\ell \mid d$.

Proof. We first prove the finite-level injection

$$S_\alpha(K)[\ell^m] \;\hookrightarrow\; \big(\operatorname{Cl}(\mathcal{O}_{L_m})[\ell^m] \otimes_{\mathbb{Z}_\ell} \mathcal{O}\big)[\beta_m], \tag{24.6}$$

where the condition on the right prescribes the action of Γ_m only. Choose $\tau \in G_K$ with $\vartheta(\tau) - 1$ a unit. This forces $D^{G_K} = 0$, so the finite lift of a given class killed by ℓ^m is unique in cohomology. Its restriction to G_{L_m} is injective. Indeed the kernel comes from a cocycle z on the abelian group Γ_m; commuting τ with σ gives $(\vartheta(\tau) - 1)z(\sigma) = (\vartheta(\sigma) - 1)z(\tau)$ there, with coefficients in R_m. Hence this cocycle is a coboundary.

Choose a primitive ℓ^m-th root to identify the restricted coefficients with roots of unity. Under Kummer theory the conjugation action on the resulting classes is $\kappa_{\ell,m}\vartheta^{-1} = \beta_m$ on Γ_m. At primes away from ℓ the restricted homomorphism vanishes on inertia. Its Kummer class has valuation divisible by ℓ^m, since passing to the maximal unramified extension preserves the value group. At each prime above ℓ the original class is zero in divisible coefficients. Its restricted finite homomorphism is therefore of the form $g \mapsto (\kappa_\ell(g)^{-r} - 1)z$ on $G_{L_{m,w}}$ for some $z \in D$, and factors through the cyclotomic image. Lemma 24.5 gives unit representatives in that completion in every coefficient coordinate. Consequently division of the principal ideal by the exponent, $(a) = \mathfrak{a}^{\ell^m} \mapsto [\mathfrak{a}]$, gives a class-group map. Its kernel consists of unit classes. Complex conjugation belongs to Γ_m since K is totally real, and $\beta_m(c) = -1$. As in Theorem 24.2, the odd part of the unit quotient is generated by roots of unity, on which τ acts by $\kappa_{\ell,m}(\tau)$. Its difference from $\beta_m(\tau)$ is a unit. The kernel meets this eigenspace in zero, proving (24.6).

Let $T = (b - \sigma_b)\Theta_{n_m}$ be the integral Stickelberger element of Theorem 24.3. It annihilates the class group of the full cyclotomic field L_m. Put $A = R_m[\Gamma_m]$. The group algebra $R_m[G_m]$ is a free A-module on any d coset representatives. Write $N(T) \in A$ for the determinant of multiplication by the reduction of T on that module. Its characteristic polynomial, applied to the element 1 by Cayley–Hamilton, shows that $N(T)$ is a multiple of T in $R_m[G_m]$. In particular it too annihilates the class group with these coefficients. On the eigenspace in (24.6), its action is the scalar obtained by evaluating Γ_m at β_m.

After this evaluation there is an explicit isomorphism of R_m-algebras

$$R_m[G_m] \otimes_{A,\beta_m} R_m \longrightarrow R_m[P], \qquad \sigma \otimes 1 \longmapsto \widetilde{\beta}_m(\sigma)[\sigma|_K].$$

It respects multiplication and sends the coset basis to a basis, each vector multiplied by a unit. The image of T is exactly $U_{b,m}$ by the floor formula for its coefficients. Formation of the determinant commutes with this base change. The resulting scalar is $B_{b,m}$, which proves the annihilation. An element of order greater than ℓ^v would give an element of order ℓ^{v+1} already in $S_\alpha(K)[\ell^m]$. This proves the exponent assertion.

Over the residue field $k = \mathcal{O}/\ell\mathcal{O}$, the augmentation ideal of $k[P]$ is nilpotent. To see this, generators g of the finite abelian ℓ-group satisfy $(g-1)^{\operatorname{ord}(g)} = 0$ in characteristic ℓ. These commuting nilpotents generate the ideal, so any product of sufficiently many generators vanishes. Multiplication by $U_{b,1}$ is multiplication by its coefficient sum plus a nilpotent endomorphism. Its determinant in dimension d is the d-th power of that sum. □

Corollary 24.10 (The residual characters left out of the determinant)**.** *On the fields E_x, take the common intervals of Corollary 19.11, with Π containing the odd primes dividing $o = \operatorname{ord}(\psi)$. At every odd prime and twist $1 \le r < t(x)$ a complementary component satisfies Theorem 24.9, except possibly for the unique character $\widetilde{\alpha} = \omega_\ell^{-r}$, where ω_ℓ is the Teichmüller cyclotomic character. At primes $\ell \nmid o$ this exceptional component vanishes. At the other odd primes the sum of its lengths over the full twist range, weighted by $\log \ell$, is at most $\exp(x^{2\varepsilon/3})$ on those same intervals.*

Proof. If the residual character is trivial on G_K, the global residual character factors through P, an ℓ-group. Its image in $k^\times$ has order prime to ℓ, hence it is globally trivial. Uniqueness of Teichmüller lifts of finite order prime to ℓ gives precisely $\widetilde{\alpha} = \omega_\ell^{-r}$, if that character factors through E_x at all. For $\ell \nmid o$ we have $K = \mathbb{Q}$, and Theorem 24.6 gives vanishing. For the finitely many remaining primes take the intervals sufficiently distant that q, d differ from each of them. The exceptional character is unramified at q, d. The two quadratic factors of $E_x/K_\psi C_l$ are generated by the inertia at these two primes: the quadratic field of discriminant $-q$ ramifies at q, and the other factors are unramified there; the same assertion holds at d. Thus $\widetilde{\alpha}$ is trivial on $H_x^0 = \operatorname{Gal}(E_x/K_\psi C_l)$. Its component lies in the H_x^0-invariants. Corollary 19.11, bounds their entire weighted sum on the common intervals. Extending scalars to the unramified $\mathcal{O}$ preserves normalized length, so it does not change that bound. □

For example, take $E = \mathbb{Q}(\zeta_7)^+(i)$, $\ell = 3$, any odd positive r, and the odd character modulo four. Here $K = \mathbb{Q}(\zeta_7)^+$ has degree three. Its inertia at three is trivial; the mod-three cyclotomic character on inertia is nontrivial, so the determinant test applies. At $m = 1$, $n_1 = 84$, $b = 5$, let u be the class of 2 in $(\mathbb{Z}/7)^\times/\{\pm 1\}$. Sorting the units j mod 84 according to the image of j^{-1} modulo seven gives the following coefficients. Each is the sum of $\lfloor 5j/84 \rfloor$ times the sign of

the character modulo four, since $r+1$ is even.

$[\sigma_j^{-1}\vert_K]$	j	coefficient before reduction
1	$1,13,29,41,43,55,71,83$	-10
u	$11,17,25,31,53,59,67,73$	2
u^2	$5,19,23,37,47,61,65,79$	0

The coefficient sum is $-8 \equiv 1 \pmod 3$, so its cube is a unit. The entire complementary component for this character vanishes, even though three divides the field degree.

For components with a nonzero determinant of valuation $v < m$, the number of cyclic summands is at most the dimension of the eigenspace in (24.6) at $m = 1$, by injection on ℓ-torsion. Multiplying this dimension by v bounds the length. The argument has removed the exclusion of whole primes from the finite test. The remaining numerical problem is to bound the sum of these lengths also where the first residue vanishes and higher determinants give poor bounds.

24.5 Finite coefficients and Kummer classes on the first cyclotomic layer

We give a test on one finite extension for each odd prime. It applies to the entire field occurring in the count, including at primes dividing its degree. The first step explains why a local condition imposed with divisible coefficients can be compared across twists using finite coefficients.

24.5.1 A description independent of the integral twist

For a number field F_0, an odd prime ℓ and a nonzero integer s, let $A_s = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-s)$, $D_{s,m} = A_s[\ell^m]$ and $G = G_{F_0,S_\ell}$. Define $\mathcal{S}_{\ell,s}(F_0)$ using the strict condition at every $w \mid \ell$ as in Volume II. Write $\Gamma = \kappa_\ell(G)$. For the absolute local Galois group at $w \mid \ell$, write $H_w = \ker(\kappa_\ell\vert_{G_{F_{0,w}}})$. Every cohomology group below uses continuous cochains on a profinite group with a discrete coefficient module.

Lemma 24.11 (Finite-level comparison)**.** *For $m \geq 1$ there is a natural isomorphism*

$$\mathcal{S}_{\ell,s}(F_0)[\ell^m] \simeq \frac{\ker\Big(H^1(G, D_{s,m}) \longrightarrow \prod_{w\mid\ell} H^1(H_w, D_{s,m})\Big)}{\inf H^1(\Gamma, D_{s,m})}. \tag{24.7}$$

In compatible cyclotomic coordinates, two nonzero twists congruent modulo $(\ell-1)\ell^{m-1}$ give the same quotient. The comparison respects the action of field automorphisms when their actions on the finite coefficients agree.

Proof. For either the global or a local cyclotomic image J, its intersection with $1+\ell\mathbb{Z}_\ell$ is an open procyclic group. This follows from finiteness of the number field or local field over $\mathbb{Q}$ or $\mathbb{Q}_\ell$, respectively, and the cyclotomic tower; globally the tower is unramified away from ℓ. If u is a topological generator of this intersection, $u^{-s} - 1 \neq 0$. Multiplication by this number is onto on $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Thus any continuous cocycle on this subgroup can be matched at the generator by a coboundary. The cocycle law and density of the integral powers give equality everywhere. The remaining quotient has order dividing $\ell - 1$, and its positive-degree cohomology vanishes by averaging. Inflation–restriction gives $H^1(J, A_s) = 0$.

Multiplication by ℓ^m on A_s is surjective, so every global class killed by ℓ^m lifts to $H^1(G, D_{s,m})$. On the kernel of the cyclotomic character both modules have trivial action. The map in degree one induced by $D_{s,m} \subset A_s$ on such a kernel is injective because it is

inclusion on homomorphisms. At $w \mid \ell$ the image in $H^1(F_{0,w}, A_s)$ is zero precisely when the finite lift restricts to zero on H_w. Indeed vanishing there makes its divisible-coefficient class inflated from the local cyclotomic image, whose degree-one cohomology just vanished. The same reasoning globally identifies the kernel of passage from finite to divisible coefficients with inflation from $H^1(\Gamma, D_{s,m})$: a class mapping to zero kills the global cyclotomic kernel, and every class inflated from Γ maps to zero. Such an inflated class belongs to the numerator. This proves (24.7). Its data involve s only through the finite character $\kappa_\ell^{-s} \bmod \ell^m$. The exponent of $(\mathbb{Z}/\ell^m)^\times$ divides $(\ell-1)\ell^{m-1}$. The assertions about congruence and automorphisms follow on cochains. □

24.5.2 The ideal class and the local generators

Let L be a CM field, let c be complex conjugation and let a minus superscript mean the image of $(1-c)/2$ on an ℓ-primary group. The group $\mathrm{Cl}(L)\{\ell\}$ denotes the ℓ-primary part of the ordinary ideal class group. Write $T_\ell(L) = \mathcal{S}_{\ell,-1}(L)^-$; here the coefficient is μ_{ℓ^∞}.

Proposition 24.12 (An injection into the ordinary class group)**.** *There is a natural injection $T_\ell(L) \hookrightarrow \mathrm{Cl}(L)\{\ell\}^-$, compatible with automorphisms commuting with c. At order dividing ℓ^m its image consists of the minus parts of the classes of fractional ideals $\mathfrak{a}$ such that $\mathfrak{a}^{\ell^m} = (z)$ for a generator satisfying*

$$z \in \mu_{\ell^\infty}(L_w)\,(L_w^\times)^{\ell^m} \qquad (w \mid \ell). \tag{24.8}$$

Proof. By the Kummer sequence and Hilbert's theorem 90 a finite lift over L is represented by $z \in L^\times/(L^\times)^{\ell^m}$. At a finite place away from ℓ this class is unramified exactly when its valuation is a multiple of ℓ^m. Indeed it becomes trivial over the maximal unramified extension precisely when a root exists there. Its value group is still $\mathbb{Z}$, and every unit has an ℓ^m-th root there by taking a root in the algebraic closure of the residue field and applying Hensel's lemma. At $w \mid \ell$ the kernel of finite-to-divisible local cohomology is the connecting image of $\mu_{\ell^\infty}(L_w)/\mu_{\ell^\infty}(L_w)^{\ell^m}$. The Kummer cocycle for such a root of unity u is $g \mapsto g(v)/v$ with $v^{\ell^m} = u$, which is exactly that connecting map. Hence strictness at w is equivalent to (24.8). This condition implies divisibility of the valuation at w as well. [3]

It follows that $(z) = \mathfrak{a}^{\ell^m}$ for a unique fractional ideal. Changing the representative of z changes $\mathfrak{a}$ by a principal ideal. Changing the finite lift of the same divisible-coefficient class multiplies z by a global root of unity modulo powers, which leaves its ideal unchanged. These observations give the map to $\mathrm{Cl}(L)[\ell^m]$ and prove the asserted description of the image after applying the minus projector. If $\mathfrak{a}$ is principal, dividing out the power of a generator lets us take z to be a global unit. For every global unit u, $u/c(u)$ is a unit of absolute value one at all complex embeddings, hence a root of unity by Kronecker's theorem. Consequently the minus part of the unit classes modulo ℓ^m-th powers is generated by roots of unity, since two is invertible there. Their prime-to-ℓ parts are already powers and their ℓ-parts die in divisible cohomology by the global connecting map. This proves injectivity on the minus part. The inclusion of finite coefficients from level m to $m+1$ sends a Kummer representative z to z^ℓ, leaving the ideal class unchanged. Passage to the union proves the full injection. All ideal and cohomology maps used commute with automorphisms. □

24.5.3 A test for every twist on the full family

Let $E/\mathbb{Q}$ be abelian and totally imaginary, $L = E(\mu_\ell)$, $\Delta = \mathrm{Gal}(L/E)$, and let ω denote the Teichmüller lift of the mod-ℓ cyclotomic character. For $r \geq 1$, put

$$M_{\ell,r}(E) = \mathcal{S}_{\ell,r}(E)^{c=(-1)^r}, \qquad T_{\ell,r}(E) = \{z \in T_\ell(L) : \sigma z = \omega(\sigma)^{r+1} z \text{ for every } \sigma \in \Delta\}.$$

Let $e_{\ell,r}(E)$ be the least nonnegative integer e such that $\ell^e T_{\ell,r}(E) = 0$. This is finite by Proposition 24.12; the same definition gives $e = 0$ for the zero group. All identifications of finite twists below use a compatible system of bases for the cyclotomic Tate module.

Theorem 24.13 (Comparison with one fixed finite group)**.** *For $1 \le m \le 1 + v_\ell(r+1)$ there is an isomorphism of finite groups*

$$M_{\ell,r}(E)[\ell^m] \simeq T_{\ell,r}(E)[\ell^m]. \tag{24.9}$$

In particular, $M_{\ell,r}(E) = 0$ exactly when $T_{\ell,r}(E) = 0$. If $v_\ell(r+1) \ge e_{\ell,r}(E)$, the entire groups in (24.9) are isomorphic without truncation. The test uses no restriction on the prime divisors of $[E : \mathbb{Q}]$.

Proof. Since $[L : E] \mid \ell - 1$, restriction identifies the strict group downstairs with the invariants upstairs. To see this globally use inflation–restriction on the absolute groups and average over Δ. At each place over ℓ, restriction on local cohomology is injective since corestriction composed with restriction multiplies by the local degree. Away from ℓ the extension is unramified and the inertia groups agree. These facts give the identification with all the local conditions.

Write any ℓ-adic unit as its Teichmüller part times a member of $1 + \ell\mathbb{Z}_\ell$. For $u \in 1 + \ell\mathbb{Z}_\ell$, binomial expansion gives $u^{r+1} \equiv 1 \pmod{\ell^{1+v_\ell(r+1)}}$, by raising successively to the ℓ-th power. Thus modulo ℓ^m the ratio of the cyclotomic character to κ_ℓ^{-r} is ω^{r+1}. On G_L this ratio is one, because L contains μ_ℓ. In the coordinates just chosen, the numerator and denominator of (24.7) over L therefore agree for exponents $-r$ and $+1$. For an automorphism of $L/\mathbb{Q}$ the action on cochains uses conjugation on the argument and the coefficient action on its value. The second action for exponent $+1$ is ω^{r+1} times the one for exponent $-r$. This factor is independent of the lift of the automorphism since $\omega|_{G_L} = 1$. Consequently the invariant classes under Δ become precisely its ω^{r+1} eigenspace. The original conjugation eigenvalue $(-1)^r$ becomes $(-1)^r(-1)^{r+1} = -1$. This proves (24.9).

Every nonzero ℓ-primary torsion group contains an element of order ℓ, so the assertion about vanishing follows by taking $m = 1$. If $a = v_\ell(r+1) \ge e = e_{\ell,r}(E)$, take $m = e + 1$. The right side is killed by ℓ^e, so the left group cannot have an element of order ℓ^{e+1}, or of any larger order. This proves the full comparison. □

Corollary 24.14 (A simultaneous length bound)**.** *On every sufficiently distant common interval of Volume IV, use its fields $E = E_x \subset \mathbb{Q}(\zeta_N)$, and set $t = \lfloor x^{401} \rfloor$. Let $\mathcal{A}_x$ consist of the pairs (ℓ, r) with ℓ odd, $1 \le r < t$, and $v_\ell(r+1) \ge e_{\ell,r}(E)$. For an absolute C,*

$$\sum_{(\ell,r)\in\mathcal{A}_x} (\log \ell)\, \mathrm{length}_{\mathbb{Z}_\ell} M_{\ell,r}(E) \le C[E : \mathbb{Q}]t^3 \log(2Nt) \le \exp(x^{\varepsilon/3}). \tag{24.10}$$

For the pairs with $\ell - 1 \mid r + 1$, the same full comparison may also be tested directly in $T_\ell(E)$ using its exponent.

Proof. Pairs with $e_{\ell,r}(E) = 0$ contribute zero by Theorem 24.13. For each contributing pair in the sum one has $\ell \mid r + 1$, hence $\ell \le t$. Its contribution is at most $\log |\mathrm{Cl}(E(\mu_\ell))|$. If $d = [E(\mu_\ell) : \mathbb{Q}]$, the conductor–discriminant formula gives $D_{E(\mu_\ell)} \le (N\ell)^d$, with $d \le [E : \mathbb{Q}]\ell$. Minkowski's bound gives representatives of norm at most $2^d D_{E(\mu_\ell)}^{1/2}$, and the sum of $(\mathrm{Norm}\,\mathfrak{a})^{-2}$ over integral ideals is at most $\zeta(2)^d$. Therefore the logarithm of the class number is at most $Cd\log(2N\ell)$. Sum over fewer than t twists and at most t primes, using $d \le [E : \mathbb{Q}]t$. On the common intervals $[E : \mathbb{Q}] \ll_\psi x^{2+8\varepsilon}$ and $\log(2N) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$. This proves the second inequality for sufficiently large x. If $\ell - 1 \mid r + 1$ then $\omega^{r+1} = 1$, so the same cochain comparison and Proposition 24.12 apply over E itself. □

Proposition 24.15 (A persistent nonzero class on the prime-count fields)**.** *For the primitive quadratic character of discriminant* -1208*, every field* E_x *in the construction has* $M_{3,r}(E_x)[3] \neq 0$ *for every positive odd* r*.*

Proof. The field cut out by the character is $F_0 = \mathbb{Q}(\sqrt{-302})$, whose ring of integers is $\mathbb{Z}[\sqrt{-302}]$, since $302 = 2\cdot 151$ is squarefree. Let $z = 73+9\sqrt{-302}$. Its norm is $73^2+81\cdot 302 = 29791 = 31^3$. A common prime divisor of (z) and $(\bar{z})$ would lie over 31 and divide $z+\bar{z} = 146$, which is impossible. As their product is $(31)^3$, it follows that 31 splits and $(z) = \mathfrak{p}^3$ for a prime of norm 31. This ideal is nonprincipal: $a^2 + 302b^2 = 31$ has no solution in integers. At every place over three, $z \in 1 + 9\mathcal{O}_{F_{0,w}}$ is a cube. Indeed for any h in that valuation ring, the polynomial $y + 3y^2 + 3y^3 - h$ has residue root $\bar{h}$ and derivative one modulo the maximal ideal. Its Hensel lift gives $(1 + 3y)^3 = 1 + 9h$.

Thus z gives a strict Kummer class of order three whose ideal class is nonzero. Conjugation sends the ideal class to its inverse because $\mathfrak{p}\bar{\mathfrak{p}} = (31)$. Its minus projection remains nonzero, so $T_3(F_0)[3] \neq 0$. For odd r, $r \equiv -1 \bmod 2$. At $m = 1$ the finite coefficient actions for $s = r, -1$ agree on the entire absolute Galois group, including conjugation. Lemma 24.11 transfers the nonzero minus class to $M_{3,r}(F_0)[3]$. Finally $[E_x : F_0]$ is a power of two. Restriction followed by corestriction multiplies the group by this power of two and therefore restriction is injective at three. The local conditions are preserved by restriction, and it commutes with conjugation. This gives the claim on the actual fields. □

The example forces positive lengths in the complementary sign even far along the common intervals. Inequality (24.10) estimates full lengths on its specified set. At the remaining pairs, (24.9) determines the first $1 + v_\ell(r+1)$ layers. Uniform control of any higher layers surviving Section 24.4 is still needed in Volume I.

24.6 Large coefficient primes and totally real class groups

On the common intervals of Section 6.6, put $t = \lfloor x^{401} \rfloor$, $b = \exp(x^\varepsilon)$ and $P = b^{1/12}$. Let $E = E_x \subset \mathbb{Q}(\zeta_N)$ be the same abelian CM field as in the theta construction. Enlarge the lower endpoint so that $P > 2t + 3$, $P > N$, and $P > [E : \mathbb{Q}]$. The last two inequalities follow from $[E : \mathbb{Q}] \ll_\psi x^{2+8\varepsilon}$ and $\log(2N) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$. Fix a prime $\ell > P$ and an unramified coefficient ring $\mathcal{O}$ containing the character values of $\mathrm{Gal}(E/\mathbb{Q})$. Write J for its fraction field and k for its residue field. For $1 \leq r < t$ and $\alpha(c) = (-1)^r$, set

$$\theta = \kappa_\ell^{-r}\alpha^{-1}, \qquad D = (J/\mathcal{O})(\theta), \qquad R_m = \mathcal{O}/\ell^m\mathcal{O}, \qquad \theta_m = \theta \bmod \ell^m.$$

Denote the strict group of Theorem 24.1 by $S_{r,\alpha}$. In this section $\mathrm{Cl}(F)\{\ell\}$ means the ℓ-primary part of the ordinary ideal class group.

Theorem 24.16 (An exact real class-group formula at every exponent)**.** *For* $m \geq 1$*, let* $F_m = (E\,\mathbb{Q}(\mu_{\ell^m}))^+$ *be the fixed field of complex conjugation and* $G_m = \mathrm{Gal}(F_m/\mathbb{Q})$*. There is an isomorphism*

$$S_{r,\alpha}[\ell^m] \;\simeq\; \mathrm{Hom}_{\mathcal{O}[G_m]}(\mathrm{Cl}(F_m)\{\ell\} \otimes_{\mathbb{Z}_\ell} \mathcal{O},\, R_m(\theta_m)). \tag{24.11}$$

The same formula holds with F_m *replaced by the cyclic totally real subfield cut out by* θ_m *and with its own Galois group and class group.*

Proof. Identify $D[\ell^m]$ with $R_m(\theta_m)$ by multiplying representatives by ℓ^m. On inertia at ℓ, $\bar{\theta} = \bar{\kappa}_\ell^{-r}$ is nontrivial: E is unramified there, and the cyclotomic image on tame inertia surjects onto $\mathbf{F}_\ell^\times$, with $0 < r < \ell - 1$. Thus D has zero invariants both globally and on the full decomposition group at ℓ. On inertia at each $p \neq \ell$ the character has finite order prime to ℓ.

Its invariants are either zero or all of D, which is divisible. The multiplication-by-ℓ^m sequence now identifies the left side of (24.11) with finite-coefficient classes unramified outside ℓ and zero on the decomposition group at ℓ. Indeed the kernel in degree one at any of these groups is its divisible-coefficient invariants modulo ℓ^m times those invariants, hence zero.

The finite character θ_m factors through G_m, since it factors through $E\mathbb{Q}(\mu_{\ell^m})$ and $\theta(c) = 1$. Write $A = R_m(\theta_m)$. Both G_m and its decomposition group at ℓ are abelian. Each contains a cyclic subgroup H of order prime to ℓ, from the tame part of inertia, on which $A^H = 0$. To see this, take the prime-to-ℓ component of an inertia element on which $\bar\theta \neq 1$. Its scalar minus one is a unit. Averaging over H gives $H^i(H, A) = 0$ for $i > 0$. The Hochschild–Serre sequence for this normal subgroup, also using $A^H = 0$, gives zero cohomology in all degrees on the two finite groups. In particular global restriction identifies $H^1(G_{\mathbb{Q}}, A)$ with the G_m-equivariant continuous homomorphisms $G_{F_m} \to A$, by inflation–restriction in degrees one and two.

For $p \neq \ell$, the inertia subgroup in G_m has order prime to ℓ, because the cyclotomic factor is unramified and $\ell \nmid [E : \mathbb{Q}]$. Its first cohomology with values in A is zero. Therefore an equivariant homomorphism comes from an unramified class at p precisely when it kills inertia over F_m there. At ℓ, the preceding vanishing on the finite decomposition group shows that the strict local condition amounts to killing the full decomposition group over F_m. Thus class field theory initially gives the ordinary class group with the primes above ℓ divided out. At infinite places the difference between narrow and ordinary class groups is 2-primary and has no effect. The relevant reciprocity theorem is the Hilbert class field theorem. J. S. Milne, *Class Field Theory*.

The classes of primes above ℓ are killed by every equivariant homomorphism in (24.11). Indeed each prime is fixed by the same tame subgroup H, since G_m is abelian. Its image must be H-invariant in A, and $A^H = 0$. This removes the quotient by those prime classes. Since A is killed by a power of ℓ, one may pass to the ℓ-primary class group and extend scalars by the tensor–Hom adjunction. The same proof applies to the field cut out by θ_m. It is totally real by evenness and is cyclic because its group is a subgroup of the product of the cyclic Teichmüller group of $k^\times$ and the cyclic group of principal rational cyclotomic units modulo ℓ^m. These factors have relatively prime orders. □

Corollary 24.17 (All prescribed twists in one class group)**.** *Write* $M_{\ell,r} = \frac{1}{2}(1+(-1)^r c)\mathcal{S}_{\ell,r}(E)$. *For every* $m \geq 1$ *one has*

$$\sum_{1\leq r<t} \operatorname{length}_{\mathbb{Z}_\ell} M_{\ell,r}[\ell^m] \leq \operatorname{length}_{\mathbb{Z}_\ell}\bigl(\mathrm{Cl}(F_m)\{\ell\}/\ell^m \mathrm{Cl}(F_m)\{\ell\}\bigr). \tag{24.12}$$

At $m = 1$ *the dimension of* $S_{r,\alpha}[\ell]$ *equals that of the* $\bar\theta$*-eigenspace in* $\mathrm{Cl}(F_1) \otimes_{\mathbb{Z}} k$. *If that eigenspace vanishes, then* $S_{r,\alpha} = 0$.

Proof. The conductors N and ℓ^m are coprime. The Chinese remainder theorem for their cyclotomic fields gives $E \cap \mathbb{Q}(\mu_{\ell^m}) = \mathbb{Q}$. Hence the prime-to-$\ell$ subgroup Δ of G_m is

$$(\mathrm{Gal}(E/\mathbb{Q}) \times \mathbf{F}_\ell^\times)/\langle (c_E, -1)\rangle,$$

using Teichmüller lifts on the cyclotomic factor. It acts on $R_m(\theta_m)$ by the reduction of $\delta_{r,\alpha}(g, z) = \alpha(g)^{-1}\tilde z^{-r}$. All these characters are distinct. Their restrictions to the second factor of the product determine r in $1 \leq r < t < \ell - 1$. Restriction to the first then determines α. Each descends to the displayed quotient by its parity.

For a character δ use the idempotent $e_\delta = |\Delta|^{-1}\sum_{\sigma\in\Delta} \delta(\sigma)^{-1}\sigma$ over $\mathcal{O}$. The homomorphisms in (24.11) factor through $e_{\delta_{r,\alpha}}$ of the class module modulo ℓ^m. The length of the module of all $\mathcal{O}$-linear homomorphisms from a finite module of exponent at most ℓ^m to R_m equals its

own length, as one sees on each cyclic summand. Equivariance can only decrease this length. The idempotents are pairwise orthogonal, so the sum is bounded by the length of the full class module modulo ℓ^m. Extension to the unramified ring $\mathcal{O}$ preserves normalized length. Applying Theorem 24.1 and summing over the complementary α's for each r gives (24.12). For $m = 1$, $G_1 = \Delta$; there is no further equivariance condition on that eigenspace, so equality holds in the single-character dimension formula. A nonzero ℓ-primary torsion group contains an element of order ℓ, which proves the vanishing assertion. □

Theorem 24.18 (A uniform sum for finite layers above $b^{1/12}$)**.** *Put $U_x = x^{-12}\exp(x^{\varepsilon}/2)$. For $\ell > P$ let*

$$m_x(\ell) = \max(\{0\} \cup \{m \geq 1 : \ell^{m+1} \leq U_x\}).$$

Then on every sufficiently distant common interval

$$\sum_{\ell > P} (\log \ell) \sum_{1 \leq r < t} \operatorname{length}_{\mathbb{Z}_\ell} M_{\ell,r}[\ell^{m_x(\ell)}] \ \ll_{\psi,\varepsilon} \ x^{-8}\exp(x^{\varepsilon}/2). \tag{24.13}$$

Here exponent $m_x(\ell) = 0$ designates the zero subgroup. This includes the entire first layer at $b^{1/12} < \ell \leq x^{-6}b^{1/4}$.

Proof. Since $\ell > b^{1/12}$, one has $\ell^6 > b^{1/2} > U_x$, so only $m = 1, 2, 3, 4$ can contribute. For each such m the field F_m has degree $d_m \leq [E : \mathbb{Q}]\ell^m$ and conductor dividing $N\ell^m$. The conductor–discriminant formula gives $|\operatorname{disc} F_m| \leq (N\ell^m)^{d_m}$. Minkowski's theorem gives an integral representative of norm at most $2^{d_m}|\operatorname{disc} F_m|^{1/2}$ in each ideal class. The number of integral ideals of norm at most Y is at most $Y^2\zeta_{F_m}(2) \leq Y^2\zeta(2)^{d_m}$, the last inequality following prime by prime. Consequently

$$\log|\operatorname{Cl}(F_m)| \ll [E : \mathbb{Q}]\ell^m \log(2N\ell^m) \ll_{\psi,\varepsilon} x^4\ell^m$$

when $\ell^{m+1} \leq U_x$. We used $[E : \mathbb{Q}] \ll_\psi x^3$, $\log(2N) \ll_{\psi,\varepsilon} x^{\varepsilon/4}$, and $\log U_x \leq x^{\varepsilon}/2$.

For primes having $m_x(\ell) = m$, the term on the left of (24.13) is at most $\log|\operatorname{Cl}(F_m)|$, by Corollary 24.17. For fixed m, the sum of ℓ^m over these primes is at most U_x: there are at most $U_x^{1/(m+1)}$ possible positive integers and each contributes at most $U_x^{m/(m+1)}$. Adding the four bounds gives $O_{\psi,\varepsilon}(x^4U_x)$, as claimed. No class-number estimate uniform in an unbounded cyclotomic exponent is used. □

The theorem bounds actual subgroups of the strict cohomology of E_x on the interval used in the theta comparison. The quotients beyond $m_x(\ell)$, including every exponent at larger primes, are still part of the required uniform estimate.

24.7 A finite class group test at the coefficient prime

Let $E/\mathbb{Q}$ be one of the abelian fields of Volume I, with conductor dividing N and degree d. Fix an odd prime $\ell \nmid Nd$. Let O be the integers of an unramified extension $J/\mathbb{Q}_\ell$ containing the character values of $\operatorname{Gal}(E/\mathbb{Q})$, and let $k = O/\ell O$. For $r \geq 1$ and a character α of $\operatorname{Gal}(E/\mathbb{Q})$ with $\alpha(c) = (-1)^r$, put

$$\vartheta = \kappa_\ell^{-r}\alpha^{-1}, \qquad M = (J/O)(\vartheta), \qquad \tau = \bar{\vartheta}, \qquad h = 1 + v_\ell(r).$$

Here κ_ℓ is the cyclotomic character and c is complex conjugation. By Theorem 24.1 the required character component on E is the group $S(\vartheta)$ of global classes in $H^1(\mathbb{Q}, M)$ unramified at $p \neq \ell$ and locally zero at ℓ. Use continuous cohomology.

Suppose first that $\tau \neq 1$. Let L be its fixed field, meaning the fixed field of its kernel, and write $\Delta = \mathrm{Gal}(L/\mathbb{Q})$. This is a totally real cyclic field in $E(\mu_\ell)$ because $\tau(c) = 1$ and $k^\times$ is cyclic. Its degree is prime to ℓ. Write $\widetilde{\tau}$ for the Teichmüller lift, the unique character of order prime to ℓ reducing to τ. For $1 \leq b \leq h$ the representations of $G_\mathbb{Q}$ on $A_b = M[\ell^b]$ and on $(O/\ell^b)(\widetilde{\tau})$ are isomorphic. Indeed $1 + \ell\mathbb{Z}_\ell$ raised to the r-th power lies in $1 + \ell^h\mathbb{Z}_\ell$, and the finite values of α are their own Teichmüller lifts.

Lemma 24.19 (The local condition before changing coefficients)**.** *Every class in $S(\vartheta)[\ell^b]$ has a unique global cohomology class lifting it in $H^1(\mathbb{Q}, A_b)$. Its unramified conditions at $p \neq \ell$ are the same at both coefficients. At ℓ, if $\tau|_{G_{\mathbb{Q}_\ell}} \neq 1$, the finite lift is locally zero. If $\tau|_{G_{\mathbb{Q}_\ell}} = 1$, its permitted restriction, under local reciprocity, is any O/ℓ^b-multiple of the homomorphism*

$$\lambda_b : \mathbb{Q}_\ell^\times \longrightarrow \mathbb{Z}/\ell^b, \qquad \lambda_b(\ell^j u) = \ell^{-1} \log\langle u \rangle \bmod \ell^b \quad (u \in \mathbb{Z}_\ell^\times). \tag{24.14}$$

Here $\langle u \rangle$ is u divided by its Teichmüller factor. These conditions on a finite class are also sufficient.

Proof. Multiplication by ℓ^b on M is surjective. In cohomology its exact sequence gives

$$0 \longrightarrow M^G/\ell^b M^G \longrightarrow H^1(G, A_b) \longrightarrow H^1(G, M)[\ell^b] \longrightarrow 0.$$

Globally the term on the left vanishes because some $\vartheta(g) - 1$ is a unit. At $p \neq \ell$ apply the same row to inertia. Its image on M is finite of order prime to ℓ. The invariants are either all of the divisible module M or zero, so again the left term vanishes. The same unit argument gives the nonsplit assertion at ℓ.

In the remaining case α is unramified at ℓ. Trivial residual action on inertia forces $\ell - 1 \mid r$. The residual unramified value of α is then one, so its local character is trivial. Thus the local action is κ_ℓ^{-r} and $M^{G_{\mathbb{Q}_\ell}} = \ell^{-h}O/O$. Indeed the local cyclotomic image is $\mathbb{Z}_\ell^\times$, and the minimum valuation of its nonzero r-th power differences from one is $1 + v_\ell(r)$. This follows by taking the logarithm on $1 + \ell\mathbb{Z}_\ell$. The boundary of $\ell^{-h}a$, using the lift $\ell^{-h-b}a$, is the homomorphism

$$g \longmapsto a\,(\kappa_\ell(g)^{-r} - 1)/\ell^h \pmod{\ell^b}.$$

In the exponential of a number in $\ell^h\mathbb{Z}_\ell$, the terms of degree at least two lie in $\ell^{2h}\mathbb{Z}_\ell$ for odd ℓ. This follows from $v_\ell(n!) \leq (n-1)/2$ for $n \geq 3$ and from the quadratic term separately. Since $b \leq h$, the boundary is a unit multiple of $a \log\langle \kappa_\ell(g) \rangle/\ell$ modulo ℓ^b. On $\mathbb{Q}_\ell^\times$, reciprocity for the cyclotomic extension kills the uniformizer and gives the unit or its inverse according to convention. Either convention gives the same line. The logarithm identifies $1 + \ell\mathbb{Z}_\ell$ with $\ell\mathbb{Z}_\ell$, so λ_b is onto. Exactness proves both directions. □

We now define a finite abelian ℓ-group $B_b(L)$. If ℓ does not split completely in L, set $B_b(L) = \mathrm{Cl}(L)\{\ell\}$. If it splits completely, identify $L_w = \mathbb{Q}_\ell$ canonically at each $w \mid \ell$ and let $B_b(L)$ be the ℓ-primary part of the following idele class quotient. Divide by $L^\times$, the full factors at infinity, the local units at finite places away from ℓ, and $\ker \lambda_b$ at each $w \mid \ell$. For $S = \{w : w \mid \ell\}$ this gives the exact sequence

$$\mathcal{O}_{L,S}^\times \longrightarrow (\mathbb{Z}/\ell^b)^S \longrightarrow B_b(L) \longrightarrow \mathrm{Cl}(\mathcal{O}_{L,S})\{\ell\} \longrightarrow 0, \tag{24.15}$$

where the first map takes the λ_b-values of the local components. To see this, first form the quotient with all $L_w^\times$ removed at $w \in S$. Fractional ideals away from S identify the result with $\mathrm{Cl}(\mathcal{O}_{L,S})$. Retaining the local quotients at S gives the indicated kernel, with precisely the relations of the global S-units. This proves finiteness and gives the sequence upon taking primary parts in the two finite groups.

Theorem 24.20 (The full strict group at the first h levels)**.** *Let*

$$C_b = e_{\widetilde{\tau}}(B_b(L) \otimes_{\mathbb{Z}_\ell} O), \qquad e_{\widetilde{\tau}} = |\Delta|^{-1} \sum_{\gamma \in \Delta} \widetilde{\tau}(\gamma)^{-1}\gamma.$$

For $1 \le b \le h$ there is an isomorphism of O-modules

$$S(\vartheta)[\ell^b] \;\simeq\; \mathrm{Hom}_O(C_b, O/\ell^b). \tag{24.16}$$

In particular $S(\vartheta) = 0$ exactly when $C_1 = 0$. In the split case this means that the $\widetilde{\tau}$-part of the S-class group at ℓ vanishes and that the projection of some S-unit to the τ-line of k^S under (24.15) is nonzero.

Proof. Restriction to G_L identifies $H^1(\mathbb{Q}, A_b)$ with Δ-equivariant continuous homomorphisms from G_L to A_b. Indeed G_L acts trivially on the coefficient module, and the outer terms of inflation–restriction vanish because $|\Delta|$ is a unit on A_b. The same averaging argument applies to each quotient of local inertia or decomposition groups. In particular, away from ℓ the homomorphism must vanish on inertia. In the nonsplit case it also vanishes on the decomposition groups at the primes above ℓ. Global class field theory then gives homomorphisms out of the ordinary ideal class group modulo the classes of those primes, as in Section 24.6. Each such prime is fixed by a decomposition subgroup containing an element on which $\tau \neq 1$, since τ is faithful on Δ. Equivariance forces its class to have zero image already.

In the split case each local map at $w \in S$ is allowed precisely the line (24.14). Equivalently it vanishes on $\ker \lambda_b$, since this local quotient is cyclic of order ℓ^b. Global reciprocity identifies all these homomorphisms with those out of the stated idele class quotient. This uses the usual local and global reciprocity maps with their compatibility under localization. [4] In both cases the targets have ℓ-power exponent. Extending scalars to O and applying the character idempotent gives (24.16). A nonzero ℓ-primary torsion group contains an element killed by ℓ. Nakayama's lemma for the finite O-module C_1 proves the vanishing criterion. In the split case Δ permutes S regularly, so the τ-part of k^S is one-dimensional. Apply the exact idempotent functor to (24.15) to obtain the last assertion. □

Corollary 24.21 (When a finite level already gives every order)**.** *The full $S(\vartheta)$ is killed by ℓ^{h-1} if and only if $C_h/\ell^h C_h$ is killed by ℓ^{h-1}. Whenever the test holds, (24.16) at $b = h$ computes its entire order and all its elementary divisors. For a fixed ℓ, α, the support and the dimension of $S(\vartheta)[\ell]$ are constant as r varies in any one class modulo $\ell - 1$ with $\tau \neq 1$.*

Proof. For a finite module over O, duality into O/ℓ^h preserves the elementary divisors of its quotient modulo ℓ^h. If the full strict group has an element of order at least ℓ^h, one of its multiples has order exactly ℓ^h, and hence occurs in $S(\vartheta)[\ell^h]$. This proves the equivalence and the assertion about orders. At $b = 1$ the field, the character idempotent and the local line depend only on τ. Reduction of κ_ℓ has order $\ell - 1$, proving the assertion about varying r. □

24.8 Vanishing for cubic residual characters

In Section 24.7, the ordinary class group of a totally real cyclic field determines whether a complementary strict component vanishes when the coefficient prime is nonsplit. For a cubic field we can bound its class number in terms of its conductor strongly enough to settle the prime-conductor case at every twist.

Lemma 24.22 (Class numbers of cyclic cubic fields)**.** *Let $L/\mathbb{Q}$ be cyclic of degree three and of conductor f. Its ordinary class number satisfies*

$$h(L) \;\le\; B(f), \qquad B(f) = \frac{f}{4}\left(\frac{\log f}{\log(f/2)}\right)^2 < f. \tag{24.17}$$

Proof. The two nontrivial characters of L are a primitive Dirichlet character χ and its conjugate, each of conductor f. They are even because they have order three. The field is totally real, and the conductor–discriminant formula gives $D_L = f^2$. Write R for the regulator with one row deleted from the logarithmic unit matrix. The residue of $\zeta_L(s) = \zeta(s)L(s,\chi)L(s,\bar\chi)$ at one and the analytic class number formula give

$$|L(1,\chi)|^2 = 4h(L)R/f.$$

The factor four is $2^3/2$, since L has three real places and its only roots of unity are $1, -1$.

Take a unit $z \neq \pm 1$. It generates L, which has prime degree. Order its three real conjugates a, b, c by decreasing absolute value. If $s = b/a$ and $t = c/b$, then $s, t \in [-1, 1]$ and

$$|(a-b)(a-c)(b-c)| = |a|^2|b|\,|(1-s)(1-t)(1-st)| \leq 2\,|a|/|c|.$$

For the inequality use $|abc| = 1$. When $s, t \geq 0$ the three factors in the second product are at most one. If just one of s, t is negative, the product is $(1-x)(1+y)(1+xy)$ with $0 \leq x, y \leq 1$, and $(1-x)(1+xy) \leq 1$. If both are negative the product is $(1+x)(1+y)(1-xy)$, which is at most $2(1+xy)(1-xy)$ because $x + y \leq 1 + xy$. These estimates give the factor two. The square of the left hand side is the discriminant of $\mathbb{Z}[z]$, equal to $D_L[\mathcal{O}_L : \mathbb{Z}[z]]^2$. Hence $\log|a| - \log|c| \geq \log(f/2)$.

The logarithmic unit lattice lies in the plane whose coordinates sum to zero. By Cauchy–Schwarz each of its nonzero vectors has length at least $\log(f/2)/\sqrt{2}$. Its covolume is $\sqrt{3}R$, since the cross product of a lattice basis is parallel to $(1,1,1)$, and each of its coordinates has absolute value R. If λ is the shortest nonzero length in any plane lattice, its covolume is at least $\sqrt{3}\,\lambda^2/2$. Indeed a shortest vector is primitive. Complete it to a lattice basis and subtract an integral multiple of it from the second vector until the parallel component has length at most $\lambda/2$. The second vector still has length at least λ, hence height at least $\sqrt{3}\,\lambda/2$. It follows here that $4R \geq \log^2(f/2)$.

Ramaré's explicit bound gives $|L(1,\chi)| \leq \frac{1}{2}\log f$ for every nonprincipal primitive even character. Its hypotheses have been checked above. Substitution proves the first inequality. A character of order three cannot have conductor at most four, since each of those unit groups has order at most two. Thus $\frac{1}{2}\log f < \log(f/2)$, giving $B(f) < f$. [5, Cor. 1] □

Theorem 24.23 (Two consequences for full primary groups)**.** *Let ℓ be an odd prime.*

1. *In the setting of Theorem 24.20, suppose the residual character τ has order three and ℓ is nonsplit in its field L. Put $f = \operatorname{cond}(L)$ and let e be the multiplicative order of ℓ modulo three. If $\ell^e > B(f)$, the entire strict group $S(\vartheta)$ vanishes. In particular $\ell^e \geq f$ suffices.*

2. *For every positive even r, if the order of ω^{-r} is at most three, then*

$$K_{2r}(\mathbb{Z})\{\ell\} = 0.$$

Here ω is the mod-ℓ cyclotomic character. The order condition is equivalent to $\ell - 1 \mid 2r$ or $\ell - 1 \mid 3r$.

Proof. In the first assertion $\ell \neq 3$, since the residue field of characteristic three has no multiplicative element of order three. Let $C = \mathrm{Cl}(\mathcal{O}_L)\{\ell\}$, and let σ generate $\mathrm{Gal}(L/\mathbb{Q})$. Extending to L the ideal norm to $\mathbb{Q}$ acts on C by $1 + \sigma + \sigma^2$, also at ramified primes. The class group of $\mathbb{Q}$ is trivial, so this operator is zero. If $C \neq 0$, the nonzero space $C/\ell C$ is consequently a module over $\mathbf{F}_\ell[X]/(X^2 + X + 1)$. Every irreducible factor of this polynomial has degree e, since its roots are the primitive cube roots of unity and Frobenius sends a root to its ℓ-th power. In

particular $\ell^e \le |C| \le h(L)$. The inequality in the hypothesis contradicts Lemma 24.22. Thus the ordinary class group has trivial ℓ-part. At a nonsplit prime the first layer of the strict group is dual to the corresponding ordinary class group component by Theorem 24.20. A nonzero ℓ-primary torsion group has an element of order ℓ, so vanishing at the first layer proves the assertion at all powers.

For the second assertion, orders one and two are covered by Proposition 20.6. Suppose the order is three. The unique cubic field L cut out by ω^{-r} is real of conductor ℓ. In the maximal real subfield $D = \mathbb{Q}(\zeta_\ell)^+$, the ω^{-r}-part of $\mathrm{Cl}(\mathcal{O}_D)/\ell$ descends to L. Indeed the subgroup fixing L has order prime to ℓ; extension followed by norm multiplies by that order, and norm followed by extension is its group sum on ideal classes. Dividing by the order gives the projector onto invariants, also after reduction modulo ℓ. By Lemma 24.22, $h(L) < \ell$, so this eigenspace is zero. The odd-prime K-group comparison of Proposition 11.19 identifies its dimension with that of $K_{2r}(\mathbb{Z})/\ell$ for even r. The group is finite, so its ℓ-part vanishes. Finally the order of ω is $\ell - 1$. Raising ω^{-r} to the second or third power gives the two divisibility conditions stated above. □

On each field E_x in Section 6.6, the second part therefore removes the indicated rational summand for all even $1 \le r < \lfloor x^{401} \rfloor$ when $\ell \nmid [E_x : \mathbb{Q}]$. The embedding as a direct summand is Corollary 11.18. For other residual character orders, and at a completely split prime in the ray class calculation, the uniform estimate still requires additional information.

24.9 Vanishing on the real quartic field of conductor sixteen

Let $C_2 = \mathbb{Q}(\zeta_{16})^+$, the real quartic layer of the cyclotomic tower used in the period field. We shall prove that the strict group on this entire subfield vanishes at every $p \equiv 3 \pmod 4$ in one congruence class of twists. These twists include positive even integers as large as the interval permits. For the rational character and $p > 3$, the corresponding cyclotomic class-group eigenspace is also the one in Osburn's Theorem 1.1. [6]

Write $\lambda(u) = (u/p)$ for the Legendre symbol of an odd prime $p \equiv 3 \pmod 4$. For a character α of $\mathrm{Gal}(C_2/\mathbb{Q})$, use its primitive Dirichlet representative, of conductor $f \in \{1, 8, 16\}$. The order-four characters are determined by their value i or $-i$ at 3 mod 16. The character $\beta = \alpha\lambda$ is primitive and odd of conductor fp, since its two factors are primitive of coprime conductors. Put

$$B(\alpha, p) = \frac{1}{fp} \sum_{a=1}^{fp} a\, \overline{\beta}(a).$$

Lemma 24.24 (A unit at the inert Gaussian prime)**.** *For the three nontrivial characters of C_2, the number $B(\alpha, p)$ lies in $\mathbb{Z}[i]$ and is a unit at the prime above p. The same holds for the trivial character if $p > 3$.*

Proof. For every character here $B(\alpha, p) = -L(0, \overline{\beta})$. Indeed, expressing the Dirichlet L-function as a sum of Hurwitz zeta functions and using $\zeta(0, z) = 1/2 - z$ gives this identity, since the complete character sum is zero. The Dirichlet functional equation for the primitive odd character relates $L(0, \overline{\beta})$ to $L(1, \beta)$ by nonzero factors, and the latter is nonzero by Dirichlet's nonvanishing theorem. Thus $B(\alpha, p) \neq 0$.

Suppose first $f = 8$ or 16. For c mod f, set

$$A(c) = \frac{1}{f} \sum_{j=0}^{f-1} j\, \overline{\alpha}(c + j).$$

Pairing j and $f-j$ and using evenness and the vanishing of the complete sum gives $A(0)=0$. The terms at $0, f/2$ vanish. Reindexing gives $A(c+1)-A(c)=\overline{\alpha}(c)$, so $A(c)$ is the partial sum of $\overline{\alpha}$ through $c-1$ for $0 \le c < f$. Every such partial sum has both real and imaginary parts in $\{-1,0,1\}$. To check this at $f=8$, the successive nonzero values of the character are $1,-1,-1,1$. At $f=16$ they are

$$1,\ -i,\ i,\ -1,\ -1,\ i,\ -i,\ 1$$

or their conjugates, in order at the odd residues $1,\dots,15$.

Write $a=u+pj$, $1 \le u < p$, $0 \le j < f$, dropping multiples of p, which contribute zero. The terms with coefficient u sum to zero at each u, as the j's run through all residues modulo f. Thus

$$B(\alpha,p)=\overline{\alpha}(p)\sum_{u=1}^{p-1}\lambda(u)A(p^{-1}u \bmod f).$$

Multiplication by $\overline{\alpha}(p)\lambda(u)$ preserves the square $[-1,1]+i[-1,1]$ and the Gaussian integer lattice. Consequently $B(\alpha,p)\in\mathbb{Z}[i]$ and the absolute value of each coordinate is at most $p-1$. As $p\equiv 3 \pmod 4$, $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a field. Divisibility by its prime above p would make both coordinates multiples of p, forcing $B(\alpha,p)=0$.

For $f=1$ and $p>3$, Euler's criterion gives $\sum_{u=1}^{p-1} u\lambda(u) \equiv \sum_{u=1}^{p-1} u^{(p+1)/2} = 0 \bmod p$. The last exponent is strictly between zero and $p-1$, so summing over the cyclic multiplicative group gives zero in $\mathbf{F}_p$. Thus $B(1,p)$ is an integer, and its absolute value is at most $p^{-1}\sum_{u=1}^{p-1} u = (p-1)/2 < p$. Its nonvanishing again proves the assertion. □

Theorem 24.25 (Full vanishing through the quartic layer)**.** *Let $p\equiv 3 \pmod 4$ be prime, and let $r\ge 1$ satisfy*

$$r+1 \equiv (p-1)/2 \pmod{p-1}. \tag{24.18}$$

Then $\mathcal{S}_{p,r}(C_2)=0$.

Proof. The twists in (24.18) are even. Since $[C_2:\mathbb{Q}]=4$, character descent in Theorem 24.1 splits the entire group after extension to an unramified ring containing i. The four strict characters over $\mathbb{Q}$ are $\theta=\kappa_p^{-r}\alpha^{-1}$. Their reflections modulo p are $\bar{\kappa}_p^{r+1}(\alpha \bmod p)$. By Euler's criterion and (24.18), the characteristic-zero lift of this finite character is $\beta=\lambda\alpha$.

For clarity, the annihilator of the first layer from Corollary 24.7 can be evaluated as an ordinary finite character sum. Set $n=fp$ and choose a positive integer a_0 coprime to n. Use the complex conjugate $\overline{\beta}=\beta^{-1}$ on units. Then

$$\sum_{a=1}^{n}\left\lfloor\frac{a_0 a}{n}\right\rfloor\overline{\beta}(a)=(a_0-\beta(a_0))B(\alpha,p). \tag{24.19}$$

Indeed, subtract the least nonnegative residue of a_0a from a_0a and divide by n. Multiplication by a_0 permutes the units, and on replacing a_0a by a new residue the character introduces the factor $\beta(a_0)$. Reducing the left side of (24.19) at the prime above p gives exactly the annihilator in (24.4) for $m=1$. That annihilation follows in Section 24.3 by sending the finite strict classes to the odd part of the cyclotomic ideal class group and applying the integral Stickelberger element.

If $\alpha\neq 1$, take $a_0\equiv 1 \bmod p$ and choose its residue modulo f so that $\alpha(a_0)\neq 1$. These two conditions are compatible by the Chinese remainder theorem. The prime-to-p root $\alpha(a_0)$ remains nontrivial modulo p. Globally the residual θ is nontrivial since the nontrivial character at conductor f cannot be cancelled by one of conductor p. Both factors on the right of (24.19) are units by Lemma 24.24. Thus $S_{\mathbb{Q}}(\theta)[p]=0$.

For $\alpha = 1,\ p > 3$, the global residual action is nontrivial since $r \equiv (p-3)/2 \bmod (p-1)$. Taking $a_0 = 2$ gives $a_0 - \lambda(a_0) \in \{1, 3\}$, a unit at p. Lemma 24.24 again applies. At $p = 3, \alpha = 1$ use $O = \mathbb{Z}_3$. The residual action is trivial, hence $F_1 = \mathbb{Q}$. In (11.6) the 3-integer class group is trivial and the single local group has order three. Thus $|B_1| \le 3$. The global boundary in (11.7) has order three by Corollary 11.23. Exactness gives $S_{\mathbb{Q}}(\theta)[3] = 0$ here as well.

Every nonzero p-primary torsion group contains a nonzero element of order p. All four strict groups therefore vanish through every power of p. Extension of scalars to the unramified coefficient ring is faithful, proving the theorem over $\mathbb{Z}_p$. □

Corollary 24.26 (A vanishing summand on every period field)**.** *Let $E = \widetilde{E}$ be the period field in Section 6.6. For all sufficiently large x on its selected intervals, $C_2 \subset E$. At every prime and twist in (24.18) with $p \equiv 3 \pmod 4$, $p \nmid [E : C_2]$ and $1 \le r < \lfloor x^{401} \rfloor$, one has*

$$\mathcal{S}_{p,r}(E)^{\mathrm{Gal}(E/C_2)} = 0.$$

Proof. The period field contains $C_{l'}$ with $l' \ge 2$ for large x. Restriction from C_2 identifies unrestricted cohomology with the invariants over E, by averaging over the relative Galois group of order prime to p. At primes over p, local restriction is injective by restriction and corestriction. At other finite primes the coefficients are unramified and an inertia homomorphism that vanishes upstairs factors through a finite group of order prime to p, hence vanishes downstairs. This gives the identification for strict groups and the conclusion follows from Theorem 24.25. □

The common field, its auxiliary primes and the interval have all been retained. This removes the indicated invariant summand also for twists outside the range of the short-subfield bound in Volume I. Components on which $\mathrm{Gal}(E/C_2)$ acts nontrivially can still contribute to the logarithmic order.

24.10 Locally trivial twists on the full real cyclotomic tower

Let p be an odd prime, $r > 0$ a multiple of $p - 1$, and $\theta = \kappa_p^{-r}$. Write $D = (\mathbb{Q}_p/\mathbb{Z}_p)(-r)$. For a number field K, let $S(K) = \mathcal{S}_{p,r}(K)$ denote the global classes unramified away from p whose restrictions to all completions above p are zero in $H^1(K_w, D)$. Put $\Sigma = \{w : w \mid p\}$. We first determine the part of $S(K)[p]$ detected at these places when the finite coefficient action is trivial.

Lemma 24.27 (Local coefficients of a strict class)**.** *Suppose $K/\mathbb{Q}$ is finite Galois and unramified at p. There is a natural sequence exact at its first two nonzero terms,*

$$0 \longrightarrow \mathrm{Hom}\big(\mathrm{Cl}(K)/\langle [w] : w \mid p\rangle, \mathbb{F}_p\big) \longrightarrow S(K)[p] \longrightarrow \mathbb{F}_p^{\Sigma}/\mathbb{F}_p\mathbf{1}. \tag{24.20}$$

The last map is equivariant for $\mathrm{Gal}(K/\mathbb{Q})$, acting by permutations on the coordinates on the right.

Proof. At each $w \mid p$ the cyclotomic character has full image $\mathbb{Z}_p^{\times}$, since $K_w/\mathbb{Q}_p$ is unramified and the local extensions generated by p-power roots of unity are totally ramified. The global image is therefore full as well. Put $b = 1 + v_p(r)$. The character θ has image $1 + p^b\mathbb{Z}_p$ locally and globally. Indeed the torsion units are killed by $p - 1 \mid r$ and the p-adic logarithm identifies the r-th power map on principal units with multiplication by r on $p\mathbb{Z}_p$. Thus

$$\lambda(g) = (\theta(g) - 1)/p^b \bmod p$$

is a homomorphism to $\mathbb{F}_p$, surjective on every decomposition group at p. It is invariant under conjugation by $G_{\mathbb{Q}}$.

By the coefficient sequence for multiplication by p on D, a strict class killed by p has a representative in $H^1(G_{K,\Sigma}, D[p])$. Identify $D[p] = p^{-1}\mathbb{Z}_p/\mathbb{Z}_p$ with $\mathbb{F}_p$ by multiplication by p on representatives. The action there is trivial, so this representative is a homomorphism $f : G_{K,\Sigma} \to \mathbb{F}_p$. On G_{K_w} it is a coboundary in D. Before identifying $D[p]$ with $\mathbb{F}_p$, this says $p^{-1}f(g) = (\theta(g) - 1)y_w$ in D for some $y_w \in D$. Since $py_w \in D^{G_{K_w}} = p^{-b}\mathbb{Z}_p/\mathbb{Z}_p$, we can write $y_w = p^{-b-1}z_w \bmod \mathbb{Z}_p$. Hence $f|_{G_{K_w}} = a_w\lambda$ with unique $a_w = z_w \bmod p$. Changing the global representative by a coboundary in D changes f by a common multiple of λ, by the same calculation with $G_{K,\Sigma}$ in place of G_{K_w}. Conversely every such multiple is a global coboundary in D. This gives the displayed map to tuples modulo constants. Both λ and the residual coefficient identification are invariant under $G_{\mathbb{Q}}$, proving equivariance.

If all a_w agree, subtract that common multiple to obtain a representative trivial on every G_{K_w}. It is unramified at every other finite place by construction. Global class field theory identifies precisely these homomorphisms with those from the ordinary class group killing the prime classes in Σ. Archimedean inertia has order at most two and has zero image since p is odd. Conversely each of these homomorphisms gives a strict class, and a global multiple of λ trivial on any one G_{K_w} must be zero. This proves exactness. □

Theorem 24.28 (Descent to a field of degree at most eight)**.** *Let $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$, $j \geq 0$. Suppose that $p \not\equiv \pm 1 \pmod{64}$ and $p - 1 \mid r$, and put*

$$a = \min\{j, v_2(p^2 - 1) - 3\}.$$

Then $0 \leq a \leq 3$, and restriction is an isomorphism of the entire strict groups $S(C_a) \simeq S(C_j)$. For every $p \equiv 3, 5 \pmod 8$ in this assertion, $S(C_j) = 0$ at every j.

Proof. By the class-number theorem of Morisawa and Okazaki, p does not divide the ordinary class number of C_j for any j whenever $p \not\equiv \pm 1 \bmod 64$ [7, Corollary B]. The prime p is unramified in C_j, so Lemma 24.27 embeds $S(C_j)[p]$ in the permutation module on the places above p, modulo its constant line. The field is abelian, so the decomposition group J of one place fixes every place above p and acts trivially on this module. It therefore acts trivially on $S(C_j)[p]$. Its order is a power of two. Averaging over J defines an idempotent on every p-primary group. If the complementary summand of $S(C_j)$ were nonzero, some element in it would have exact order p, by multiplying an element of finite p-power order. All classes have finite p-power order since a continuous cocycle from a compact group to D has finite image. This contradicts triviality of J on $S(C_j)[p]$. Thus the full group is J-invariant.

For a Galois extension of degree prime to p, restriction identifies the lower strict group with the invariants of the upper strict group. Indeed inflation–restriction for the absolute Galois groups gives an isomorphism on global H^1 with those invariants, since positive-degree cohomology of the finite quotient on p-primary modules vanishes by averaging. Local restriction at p is injective by restriction and corestriction. At a prime away from p the coefficients are unramified. An inertia homomorphism vanishing after restriction factors through a finite quotient of order prime to p, so vanishes. This proves descent with all the stated local conditions.

The cyclic group of C_j is $(\mathbb{Z}/2^{j+2}\mathbb{Z})^\times/\{\pm 1\}$, and J is generated by p in this quotient. Choose the sign $u = \pm p$ with $u \equiv 1 \bmod 4$, and put $e = v_2(u - 1)$. Then $e = v_2(p^2 - 1) - 1$ because the other of $p - 1, p + 1$ has valuation one. Successive squaring of u increases the valuation of its difference from one by exactly one each time, as $u^{2^d} + 1 \equiv 2 \bmod 4$. Its order in the cyclic quotient is $2^{\max(0, j+2-e)}$. Hence J has index $2^{\min(j, e-2)} = 2^a$, and its fixed field is C_a. Our condition modulo 64 gives $e \leq 5$. This proves the isomorphism. If $p \equiv 3, 5 \bmod 8$, then $e = 2$, $a = 0$, and Σ consists of a single place in C_j. The permutation quotient is zero. The injection above gives $S(C_j)[p] = 0$, so $S(C_j) = 0$. □

Corollary 24.29 (The cyclotomic contribution on the period field)**.** *Take the actual period field $E = K_\psi C_{l'}(\sqrt{-q}, \sqrt{-d_0})$ on the intervals of Section 6.6. Put $A = \mathrm{Gal}(E/C_{l'})$, $m_E = |A|$, and take a in Theorem 24.28 with $j = l'$. Under its hypotheses,*

$$m_E\, S(E)^A \;\subset\; \mathrm{res}_{E/C_a}\, S(C_a).$$

If $p \nmid m_E$, restriction identifies $S(C_a)$ with $S(E)^A$. For $p \equiv 3, 5 \bmod 8$ one has $m_E\, S(E)^A = 0$ even when $p \mid m_E$. In those residue classes and twists the invariant part contributes zero after multiplication by the depth $p^{k_{p,r}}$ of Theorem 19.19, for every sufficiently large x on the same intervals.

Proof. Corestriction takes $S(E)$ to $S(C_{l'})$. At the primes over p this follows from the local restriction–corestriction formula and the strict zero restrictions upstairs. At each other finite prime apply the same double-coset formula on inertia. Every upper restriction there is zero, by unramifiedness of both the coefficients and the class. Restriction back to E is the sum of the A-translates, hence is multiplication by m_E on $S(E)^A$. Apply Theorem 24.28 and, when $p \nmid m_E$, prime-to-p descent as in its proof.

For the last claim $m_E \le 4[K_\psi : \mathbb{Q}]$ on all the intervals. Only the primes dividing an integer of this bounded size can give a nonzero invariant group in these residue classes. For all such p the depth $k_{p,r}$ tends to infinity uniformly for $1 \le r < \lfloor x^{401} \rfloor$ by Theorem 19.19. In particular it exceeds $v_p(m_E)$ for all sufficiently large x. This kills $S(E)^A$ at that depth. □

For example all positive even twists at $p = 3$ satisfy the vanishing on $C_{l'}$, uniformly up to the terminal twist of the period construction. The other character components on E and coefficient primes outside the given congruences remain in the full interval estimate.

25 Special values and integral annihilators

25.1 Strict classes and finite even K-groups

Let E be a totally imaginary number field of degree d. For $r \ge 1$ and any prime ℓ write

$$M = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)(-r), \qquad \mathcal{S}_{\ell,r}(E) = \ker\left(H^1(G_{E,S}, M) \longrightarrow \prod_{v \mid \ell} H^1(E_v, M) \right).$$

Here S contains the places above ℓ and the archimedean places, and $G_{E,S}$ permits ramification only in S. For this definition take no other finite places in S. For $K = E$ or one of the completions E_v above ℓ let $w_{\ell,r}(K) = |H^0(K, M)|$. Use $K_j(\mathcal{O}_E)$ for Quillen's algebraic K-groups, $B\{\ell\}$ for the ℓ-primary subgroup of an abelian group, and $B^\vee$ for its Pontryagin dual. The strict group is the group in Section 6.4.

Theorem 25.1 (The strict kernel in an even K-group)**.** *There is a natural exact sequence*

$$\begin{aligned} 0 \longrightarrow \mathcal{S}_{\ell,r}(E)^\vee \longrightarrow K_{2r}(\mathcal{O}_E)\{\ell\} \longrightarrow \bigoplus_{v \mid \ell} H^0(E_v, M)^\vee \\ \longrightarrow H^0(E, M)^\vee \longrightarrow 0. \end{aligned} \tag{25.1}$$

In particular each strict group is finite. For fixed E, r only finitely many coefficient primes contribute. For all of them, including two,

$$|\mathcal{S}_{\ell,r}(E)| = |K_{2r}(\mathcal{O}_E)\{\ell\}|\, \frac{w_{\ell,r}(E)}{\prod_{v \mid \ell} w_{\ell,r}(E_v)}. \tag{25.2}$$

Proof. For $j \geq 1$ use the finite dual modules $A_j = M[\ell^j]$ and $B_j = \mathbb{Z}/\ell^j(r+1)$, paired into μ_{ℓ^j}. Let $\mathrm{Sha}^i_S(C)$ in this proof denote the kernel of restriction in degree i from $G_{E,S}$ to the places in S, with the usual Tate modification at infinity. The complex places have zero modified groups. Finite-module Poitou–Tate duality pairs $\mathrm{Sha}^1_S(A_j)$ perfectly with $\mathrm{Sha}^2_S(B_j)$. The last part of its sequence identifies the cokernel of $H^2(G_{E,S}, B_j) \to \bigoplus_{v|\ell} H^2(E_v, B_j)$ with $H^0(E, A_j)^\vee$. Local Tate duality identifies these local degree-two groups with $H^0(E_v, A_j)^\vee$. The hypotheses for duality hold since all primes dividing the orders of the modules are in S. [8, I, Cor. 2.3 and Thm. 4.10]

The inclusions $A_j \to A_{j+1}$ correspond under the pairings to the quotient maps $B_{j+1} \to B_j$. Continuous cohomology of discrete modules commutes with this direct limit. The product of local groups here is finite in the number of factors. Exactness of the direct limit gives $\varinjlim_j \mathrm{Sha}^1_S(A_j) = \mathcal{S}_{\ell,r}(E)$. Take the inverse limit on the dual side. The finite global and local cohomology groups of the B_j satisfy the Mittag–Leffler condition, since their images stabilize at each fixed index. Inverse limits of the resulting exact systems of finite groups are exact. In particular the degree-one inverse-limit correction in continuous degree two vanishes. The global middle term in (25.1) at this stage is $H^2(G_{E,S}, \mathbb{Z}_\ell(r+1))$.

We use the number-ring comparison theorem in its even-degree form. For $r \geq 1$, if ℓ is odd or the field is totally imaginary, it identifies $K_{2r}(\mathcal{O}_E)\{\ell\}$ with $H^2_{\mathrm{et}}(\mathcal{O}_E[1/\ell], \mathbb{Z}_\ell(r+1))$. The latter is $H^2(G_{E,S}, \mathbb{Z}_\ell(r+1))$ by comparison with restricted-ramification Galois cohomology for ℓ-primary coefficients on this ring. In the comparison the residue fields at $v \mid \ell$ contribute no ℓ-primary change upon inverting ℓ. Their positive even K-groups vanish and their group in degree $2r-1$ has order $|\kappa(v)|^r - 1$, prime to ℓ. The even global group is finite by the finite-generation theorem for rings of integers and Borel's rank formula. [9, Ch. VI, Thms. 8.2 and 8.4] These results apply here also at two. Substitution gives (25.1). Finiteness of the middle group gives finite support in ℓ, and taking orders gives (25.2). □

Lemma 25.2 (The local correction)**.** *Put $d_v = [E_v : \mathbb{Q}_\ell]$. Then $w_{\ell,r}(E_v) \leq 4rd_v$. For odd $\ell > rd_v + 1$ it equals one. At an odd prime unramified in E, the correction $\sum_{v|\ell} \log w_{\ell,r}(E_v) - \log w_{\ell,r}(E)$ is exactly*

$$\begin{cases} (g_\ell - 1)(1 + v_\ell(r)) \log \ell, & \ell - 1 \mid r, \\ 0, & \ell - 1 \nmid r, \end{cases}$$

where g_ℓ is the number of places above ℓ.

Proof. The cyclotomic image of G_{E_v} has index j_v in $\mathbb{Z}_\ell^\times$ equal to the degree over $\mathbb{Q}_\ell$ of $E_v \cap \mathbb{Q}_\ell(\mu_{\ell^\infty})$. This index divides d_v. The image contains all j_v-th powers. An element of exact order ℓ^a in M is fixed precisely when the r-th powers of the image are one modulo ℓ^a. Hence the exponent of $(\mathbb{Z}/\ell^a)^\times$ divides rj_v. For odd ℓ and $a \geq 1$ this exponent is $(\ell-1)\ell^{a-1}$. It follows that $\ell \leq rd_v + 1$ and $\ell^a \leq 2rd_v$. For $\ell = 2$, $a \geq 3$ the exponent is 2^{a-2}, yielding $2^a \leq 4rd_v$. The smaller exponents obey the same bound. Since M has one subgroup of each ℓ-power order, these bounds apply to the full group of invariants.

If v is unramified over ℓ, the totally ramified cyclotomic tower intersects E_v trivially over $\mathbb{Q}_\ell$. Its local image is therefore all of $\mathbb{Z}_\ell^\times$. The global image contains this image of a decomposition group, so it too is full. For odd ℓ, the largest a such that $(\ell-1)\ell^{a-1} \mid r$ is $1 + v_\ell(r)$ if $\ell - 1 \mid r$, and there is no such $a \geq 1$ otherwise. This gives the asserted difference of logarithms. □

Corollary 25.3 (An exact sum and a polynomial error on the common fields)**.** *For $t \geq 2$ an integer let $\mathcal{L}_E(t)$ be the supremum over finite sets of primes of $\sum_\ell (\log \ell) \sum_{1 \leq r < t} \mathrm{length}_{\mathbb{Z}_\ell} \mathcal{S}_{\ell,r}(E)$*

restricted to the chosen set. Then

$$\mathcal{L}_E(t) = \sum_{1\le r<t} \log|K_{2r}(\mathcal{O}_E)| - C_E(t), \tag{25.3}$$

$$C_E(t) = \sum_{1\le r<t} \sum_{\ell} \left(\sum_{v\mid \ell} \log w_{\ell,r}(E_v) - \log w_{\ell,r}(E) \right),$$

$$0 \le C_E(t) \ll d^2 t^2 \log(4dt).$$

For $E = E_x$, $t = \lfloor x^{401} \rfloor$ from Volume I, this error is $o(\exp(x^{\varepsilon}/2))$, uniformly as the common intervals recede.

Proof. For a finite ℓ-group B, its length times $\log \ell$ is $\log|B|$. Theorem 25.1 gives finitely many nonzero groups for the finitely many r, so the supremum is attained. Sum its order formula over all primes and twists. Restriction embeds the global invariants in each local set of invariants, so each correction is nonnegative. By Lemma 25.2, only primes $\ell \le dr+1$ need be counted, including two. There are at most d places at each, and their total logarithm is at most $d\log(4dr)$. Summing over $r < t$ gives the displayed error bound. The degree $[E_x : \mathbb{Q}]$ is bounded by a fixed power of x on the intervals, whence the last assertion. □

The fixed-scale finiteness assertion was also proved in Section 11.2. Formula (25.3) expresses the entire strict sum in finite global groups on E_x itself. It supplies the correction to be subtracted when using bounds on their orders. Uniform control of the sum of those orders' logarithms at the precision of Volume I, equation (L), is still needed.

25.2 Special values and the two conjugation eigenspaces

Let $E/\mathbb{Q}$ be a CM abelian extension of conductor dividing N, let $F = E^+$ be its maximal real subfield, and put $f = [F : \mathbb{Q}]$ and $d = 2f$. Suppose that E/F is unramified at all finite places. These hypotheses hold for the fields E_x of Theorem 94.9. Indeed, complex conjugation c acts nontrivially on the two imaginary quadratic subfields of coprime discriminants $-q_0, -d_0$. At each rational prime inertia is trivial on at least one of them. Thus c lies in no finite inertia group.

For $m \ge 2$ let $B_m^{\delta}(E)$, with $\delta = +1$ or -1, be the δ-eigenspace of c on the subgroup of elements of odd order in $K_{2m-2}(\mathcal{O}_E)$. Write $w_m(J) = |H^0(J, (\mathbb{Q}/\mathbb{Z})(m))|$ for a number field J. Let X be the characters of $\mathrm{Gal}(E/\mathbb{Q})$, each represented by its primitive Dirichlet character. Define

$$X_m = \{\chi \in X : \chi(c) = (-1)^m\}, \qquad P_m = \prod_{\chi \in X_m} L(1-m, \chi).$$

There are f characters of each sign. This follows by restriction to $\langle c \rangle$ in the character group of a finite abelian group. Section 11.1 bounded the corresponding sign of the strict kernels. Here we determine the odd order of the full global eigenspace before imposing any local condition.

Lemma 25.4 (One common denominator for the special values)**.** *Let $D_m = mN(m+1)!$. The number $D_m^f P_m$ is a nonzero rational integer, and*

$$\log|D_m^f P_m| \ll fm \log(2mN).$$

Proof. Define $B_j(z)$ by $ue^{zu}/(e^u - 1) = \sum_{j\ge 0} B_j(z) u^j/j!$. For a primitive character of conductor $q \mid N$, the exponential sum at $y > 0$ equals $\sum_{a=1}^{q} \chi(a) e^{-ay}/(1-e^{-qy})$. Its Mellin integral is $\Gamma(s)L(s,\chi)$ for $\mathrm{Re}\, s > 1$. At zero the coefficient of y^{m-1} is $q^{m-1}\sum_a \chi(a) B_m(1-a/q)/m!$. Subtract the Laurent terms through that degree on $(0,1]$ before integrating. The integral of

the remainder is holomorphic at $s = 1-m$, as is the exponentially convergent integral on $[1,\infty)$. Each subtracted monomial by^j contributes $b/(s+j)$. Divide the resulting residue at $1-m$ by that of $\Gamma(s)$, which is $(-1)^{m-1}/(m-1)!$. Replacing u by $-u$ gives $B_m(1-z) = (-1)^m B_m(z)$. Together these calculations give

$$L(1-m,\chi) = -\frac{q^{m-1}}{m}\sum_{a=1}^{q}\chi(a)B_m(a/q).$$

The formula also applies at $q=1$ with $\chi(1)=1$.

Put $B_j = B_j(0)$. Multiplication of the generating series by $e^u - 1$ gives $B_0 = 1$ and $(j+1)B_j = -\sum_{i<j}\binom{j+1}{i}B_i$ for $j \geq 1$. Induction gives $(j+1)!B_j \in \mathbb{Z}$. In the expansion $B_m(z) = \sum_{j=0}^{m}\binom{m}{j}B_j z^{m-j}$, multiplication by q^{m-1} clears the denominator from $z = a/q$ except possibly one factor q. Hence $D_m L(1-m,\chi)$ is an algebraic integer. The Galois group of the cyclotomic field of character values permutes the characters in X_m and preserves their conductors. The product of the cleared values is therefore a rational integer.

For $\chi \in X_m$, the gamma factor in the Dirichlet functional equation is finite and nonzero at $1-m$, since χ has the parity of m. The Euler product at $m > 1$ is nonzero, so $L(1-m,\chi) \neq 0$. Finally the Bernoulli generating function is bounded by an absolute constant on $|u| = 1,\ 0 \leq z \leq 1$. Cauchy's estimate gives $|B_m(z)| \leq Cm!$. It follows that $|L(1-m,\chi)| \leq C(m-1)!N^m$. Multiply over the f characters and use $\log(m!) \leq m\log m$. □

Theorem 25.5 (The order of the critical eigenspace)**.** *Set $J = F$ if m is even and $J = E$ if m is odd. For every odd prime ℓ one has*

$$v_\ell|B_m^{(-1)^m}(E)| = v_\ell(w_m(J)|P_m|)\,.$$

In particular, with an absolute implicit constant,

$$\log|B_m^{(-1)^m}(E)| \ll dm\log(4dmN), \tag{25.4}$$
$$\sum_{r=1}^{t-1}\log|B_{r+1}^{(-1)^{r+1}}(E)| \ll dt^2\log(4dtN) \qquad (t \geq 2).$$

Proof. Fix $\ell > 2$. The comparison used in Theorem 25.1 applies to E and, at this odd prime, also to F. The quadratic extension is unramified away from the infinite places. On the rings with ℓ inverted it is an étale Galois cover. Restriction identifies $H^2(\mathcal{O}_F[1/\ell],\mathbb{Z}_\ell(m))$ with the invariants of $H^2(\mathcal{O}_E[1/\ell],\mathbb{Z}_\ell(m))$, where cohomology is étale. Indeed all positive cohomology of the covering group on ℓ-primary coefficients vanishes by averaging. Apply Hochschild–Serre at finite coefficients and take inverse limits as in Theorem 25.1. Thus the plus group has the odd local order of $K_{2m-2}(\mathcal{O}_F)$, and the minus group has the quotient of the two local orders for E and F.

If $m = 2k$, the abelian totally real special-value theorem gives

$$v_\ell|\zeta_F(1-m)| = v_\ell|K_{4k-2}(\mathcal{O}_F)| - v_\ell|K_{4k-1}(\mathcal{O}_F)|.$$

This is the odd part of the theorem in [9, Ch. VI, Thms. 8.7–8.8]. We verify that $v_\ell|K_{4k-1}(\mathcal{O}_F)| = v_\ell w_m(F)$. The group $K_{4k-1}(\mathcal{O}_F)$ has rank zero by Borel's theorem. At this prime its completion is $H^1(\mathcal{O}_F[1/\ell],\mathbb{Z}_\ell(m))$ by the same number-ring comparison. The coefficient sequence from $\mathbb{Z}_\ell(m)$ to $\mathbb{Q}_\ell(m)$ identifies the torsion of this group with $H^0(F,\mathbb{Q}_\ell/\mathbb{Z}_\ell(m))$. The preceding rational invariants vanish since the cyclotomic image is open and $m > 0$. The rational degree-one cohomology is a vector space, so the connecting map has exactly the stated torsion image.

If m is odd, then $m \geq 3$. Write ξ for the quadratic character of E/F. The higher relative class number formula gives, at odd ℓ,

$$v_\ell\Big(\frac{|K_{2m-2}(\mathcal{O}_E)|}{|K_{2m-2}(\mathcal{O}_F)|}\Big) = v_\ell(w_m(E)|L(1-m,\xi)|)\,.$$

In this formula the higher class numbers are the orders of degree-two integral étale cohomology and agree with the indicated K-group orders at odd primes. The higher unit index and the explicit power of two have zero valuation at ℓ. This is the odd-prime conclusion of the CM special-value theorem, which is unconditional for every CM quadratic extension of a totally real field. [10, Prop. 1.3]

The abelian factorization of ζ_E gives $P_m = \zeta_F(1-m)$ in even weight and $P_m = L(1-m,\xi)$ in odd weight. Indeed the characters trivial on $\mathrm{Gal}(E/F)$ are precisely the even characters. At a rational prime the local factors are computed on the inertia invariants of these characters, which gives their primitive Euler factors, including at the ramified primes. The identity for $L(s,\xi)$ follows on the half-plane of absolute convergence by dividing $\zeta_E(s)$ by $\zeta_F(s)$, and then by continuation of the product of odd characters. This proves the valuation formula in both parities.

For $J = E$ or F, the index of its cyclotomic image in $\mathbb{Z}_p^\times$ divides $[J:\mathbb{Q}] \leq d$. If a twisted invariant has order p^a, the exponent of $(\mathbb{Z}/p^a)^\times$ divides m times this index. As in Lemma 25.2, one obtains $p^a \leq 4dm$ and $p \leq dm+1$. Hence $\log w_m(J) \ll dm\log(4dm)$. By Lemma 25.4, $w_m(J)D_m^f P_m$ is a nonzero integer. At every odd prime its valuation is the group valuation in the statement plus $f v_\ell(D_m)$. Thus the odd group order divides the absolute value of this integer. The lemma bounds its logarithm and gives (25.4). Summing over $m = 2,\dots,t$ gives the second estimate. □

In particular, on the intervals of Volume I the full range $1 \leq r < \lfloor x^{401} \rfloor$ contributes only $x^{O(1)}$ to the logarithms in (25.4). Here $d \ll_\psi x^3$ and $\log(2N) \ll_{\psi,\varepsilon} x$ on the chosen fields. The eigenspace with sign $(-1)^r$ at twist r still requires a bound of its own.

25.3 Bernoulli sums for characters at every two-power layer

Let $p \equiv 3 \pmod 4$, and write $\lambda(u) = (u/p)$. For a primitive even character α of order 2^j of the real cyclotomic tower, $j \geq 1$, its conductor is $f = 2^{j+2}$. Put $D_j = 2^{j-1}$, $L_j = \mathbb{Q}(\zeta_{2^j})$, and $n = fp$. The quantity

$$B_\alpha = \frac{1}{n}\sum_{v=1}^{n} v\,\overline{\alpha\lambda}(v) = -L(0,\overline{\alpha\lambda})$$

is the same Bernoulli sum as in Section 24.9. The character $\alpha\lambda$ is primitive and odd, so the functional equation and nonvanishing at one give $B_\alpha \neq 0$. Let $F_j(p)$ denote the residue degree of p in L_j, including $F_1(p) = 1$.

Lemma 25.6 (Integral coordinates and norms)**.** *Write $B_\alpha = \sum_{t=0}^{D_j-1} b_t \zeta_{2^j}^t$. Then $b_t \in \mathbb{Z}$ and $|b_t| \leq p-1$ for every t. At least one prime above p has valuation zero on B_α. With valuations normalized by $v_\mathfrak{p}(p) = 1$, one has*

$$F_j(p)\sum_{\mathfrak{p}\mid p} v_\mathfrak{p}(B_\alpha) \leq D_j \log_p\big((p-1)\sqrt{D_j}\big), \tag{25.5}$$

$$F_j(p)\sum_{\mathfrak{p}\mid p} v_\mathfrak{p}(B_\alpha) \leq D_j \log_p\left(\frac{\sqrt{fp}}{\pi}\big(2+\log(fp)\big)\right). \tag{25.6}$$

Here $\log_p y = \log y/\log p$ is a real logarithm.

Proof. For an integer c modulo f use the partial sum

$$A(c) = \frac{1}{f} \sum_{v=0}^{f-1} v\, \bar{\alpha}(c+v).$$

Evenness and the vanishing of the complete character sum give $A(0) = 0$ by pairing v and $f - v$. A shift of the summation index gives $A(c+1) - A(c) = \bar{\alpha}(c)$. For $0 \le c < f$ this is the sum of the first c character values.

Each coordinate of every such sum in the displayed power basis is $0, 1$, or -1. To see this, the even character of exact order 2^j is faithful on $(\mathbb{Z}/f\mathbb{Z})^\times/\{\pm 1\}$. Its kernel on the units has order two, and $\alpha(1 + f/2) = -1$ by primitivity. The residues contributing to any fixed basis coordinate occur in a four-element set. Writing its least residue as a gives

$$0 < a < f/4, \qquad a, \quad f/2 - a, \quad f/2 + a, \quad f - a.$$

Indeed the two operations are negation and translation by $f/2$, the latter coinciding on odd residues with multiplication by $1 + f/2$. The four signs in increasing order are $(+, -, -, +)$ up to overall sign. Every partial sum of those signs is $0, 1$ or -1, proving the assertion.

Write a residue prime to p as $u + pv$ with $1 \le u < p$, $0 \le v < f$, and sum first in v. The part weighted by u has zero sum since $\alpha \ne 1$. One obtains

$$B_\alpha = \bar{\alpha}(p) \sum_{u=1}^{p-1} \lambda(u) A(p^{-1}u \bmod f).$$

A sign times a 2^j-th root of unity permutes the power basis up to signs, since $\zeta^{D_j} = -1$. This proves the coordinate bound in the integral basis of L_j. If all primes above p divided B_α, then B_α would lie in $p\mathcal{O}_{L_j}$, since p is unramified. Every coordinate would be divisible by p, forcing them all to be zero. This contradicts nonvanishing.

The average of $|\sigma B_\alpha|^2$ over the embeddings of L_j is $\sum_t b_t^2$. Indeed the average of $\sigma(\zeta)^{t-t'}$ over the odd powers of ζ vanishes for $0 < |t - t'| < D_j$ by a geometric sum. The geometric mean of $|\sigma B_\alpha|$ is therefore at most $(p-1)\sqrt{D_j}$. The left side of (25.5) is the p-adic valuation of the absolute rational norm. This proves (25.5). For a primitive odd character β modulo n, evaluating its completed functional equation at zero gives $|L(0, \bar{\beta})| = \sqrt{n}\, |L(1, \beta)|/\pi$. The series for $L(1, \beta)$ through n has absolute value at most $1 + \log n$, and the absolute value of its tail is at most one by summation by parts with partial sums bounded by n. Apply this at each embedding to prove (25.6). □

Theorem 25.7 (Components of the strict group at all layers)**.** *Suppose $p > 3$, $p \equiv 3 \pmod 4$, and $r + 1 \equiv (p-1)/2 \bmod (p-1)$. For every $j \ge 1$, at least one full Frobenius orbit of the primitive characters of order 2^j has zero strict component on C_J for every $J \ge j$. The same orbit works for all the indicated twists. For $p \equiv 3 \bmod 8$ and $J \ge 2$, at least $2^{J-1} + 2$ of the 2^J character labels of C_J have zero component.*

For a fixed p-adic embedding attached to $\mathfrak{p} \mid p$ put $b_\alpha = v_\mathfrak{p}(B_\alpha)$. If $b_\alpha < 1 + v_p(r+1)$, the strict component for that embedding is killed by p^{b_α}.

Proof. Extend coefficients to an unramified ring containing the character values. Descent from C_J to $\mathbb{Q}$ separates the characters by Theorem 24.1, since the degree of C_J is a power of two. For $\alpha \ne 1$, the residual character $\bar{\kappa}_p^{-r}\bar{\alpha}^{-1}$ is globally nontrivial by its conductor at two. The twist r is even. The reflection test (24.4) applies with the primitive conductor f, as in Section 24.9. Put $m = 1 + v_p(r+1)$. At level p^m, every unit v satisfies $v^{r+1} = \lambda(v) \bmod p^m$. In fact $r + 1$

kills its principal unit part modulo p^m, and on the Teichmüller part its power is exactly the Legendre symbol.

Choose $a_0 \equiv 1 \bmod p$ with $\alpha(a_0) \neq 1$ at conductor f by the Chinese remainder theorem. The scalar $a_0 - (\alpha\lambda)(a_0)$ is a p-adic unit since a nontrivial root of unity of two-power order stays nontrivial in residue characteristic p. At modulus fp^m the floor sum in (24.4) is congruent to $(a_0 - (\alpha\lambda)(a_0))B_\alpha$. To check the change of modulus, lift each unit modulo fp to its p^{m-1} representatives modulo fp^m. The sum of their least positive residues divided by fp^m is the original residue divided by fp, plus $(p^{m-1}-1)/2$. The additional term sums to zero against the nontrivial character. Now permute units by multiplication by a_0, as in (24.19), to obtain the identity for floors. Thus if $b_\alpha < m$, the test kills the p^m-torsion by p^{b_α}. Any element of greater order would yield an element of order exactly $p^{b_\alpha+1}$ by multiplication by a power of p, a contradiction. This proves the exponent bound, including vanishing for $b_\alpha = 0$.

All the primitive labels of order 2^j are conjugates of α. The quadratic character λ is rational, so $B_{\sigma\alpha} = \sigma B_\alpha$ under these conjugations. In a fixed p-adic closure the conjugate labels run through all primes of L_j above p, with one orbit of size $F_j(p)$ for each prime. Lemma 25.6 supplies at least one unit orbit. For $p \equiv 3 \bmod 8$ and $j \geq 3$, $F_j(p) = 2^{j-2}$, since $v_2(p^2-1) = 3$ and successive squaring adds one to this valuation. The four labels through order four all vanish by Theorem 24.25. Adding $4 + \sum_{j=3}^{J} 2^{j-2}$ proves the stated count. □

Corollary 25.8 (Uniform exponents at selected twists)**.** *Let $p > 3$, $p \equiv 3 \bmod 8$, $J \geq 2$, and assume the twist congruence of Theorem 25.7. If*

$$v_p(r+1) \;\geq\; 1 + \lceil \log_p(2^J) \rceil,$$

then the whole group $S(C_J)$ is killed by $p^{\lceil 2+\log_p(2^J)\rceil}$. If instead

$$p > 2^{J+2}\big(2 + \log(2^{J+2}p)\big)^2, \qquad p \mid r+1,$$

then $pS(C_J) = 0$.

Proof. The components through order four already vanish. At every remaining layer $D_j/F_j(p) = 2$. From (25.5), $b_\alpha < 2 + \log_p D_j$, so the first hypothesis puts b_α strictly below $1 + v_p(r+1)$ for every label. For the second assertion $\sqrt{fp}(2 + \log(fp))/\pi < p$ for all conductors $f \leq 2^{J+2}$. Thus (25.6) gives $\sum_{\mathfrak{p}\mid p} v_{\mathfrak{p}}(B_\alpha) < 2$. Every b_α is a nonnegative integer and is at most one. Apply Theorem 25.7 and descend the bounds from the faithfully flat unramified coefficient extension. □

25.4 An integral annihilator across the twists

Let $E/\mathbb{Q}$ be a finite abelian field, $n = [E : \mathbb{Q}]$, of conductor dividing N. Let p be odd, $p \nmid n$, and choose a character α of $\mathrm{Gal}(E/\mathbb{Q})$ with values in an unramified coefficient ring O over $\mathbb{Z}_p$. Write $\alpha = \alpha'\omega^i$ on the units of its conductor times p, where α' is primitive of conductor f prime to p, and ω is the Teichmüller character at p. This factorization follows by the Chinese remainder theorem. The order of α divides n, so its local factor at p is trivial on the principal units. Fix $r_0 \bmod (p-1)$ with $\alpha(-1) = (-1)^{r_0}$, and write $h = r_0 + 1 + i \bmod (p-1)$. For $r > 0$ in this residue class denote the strict component over $\mathbb{Q}$ for $\kappa_p^{-r}\alpha^{-1}$ by $S_{\alpha,r}$. If its residual character is trivial, Theorem 24.6 already gives $S_{\alpha,r} = 0$. The following calculation applies to the other components, including those ramified at p.

Theorem 25.9 (An interpolating annihilator and a nonzero value)**.** *Set $b = 1 + fp$, and take the unique $j \in \{1, \dots, p-1\}$ with $j \equiv -h \bmod (p-1)$. There is a power series $\mathcal{A}(X) = \sum_{d\geq 0} c_d X^d$ over O, convergent on $\mathbb{Z}_p$, with the following properties.*

1. *$v_p(c_d) \geq d - v_p(d!)$. For every $m \geq 1$, the value $\mathcal{A}(r+1) \bmod p^m$ annihilates $S_{\alpha,r}[p^m]$.*
2. *With $k = j+1$, $\chi = \bar{\alpha}'$ and $B_{k,\chi} = f^{k-1}\sum_{a=1}^{f}\chi(a)B_k(a/f)$, one has*

$$\mathcal{A}(-j) = \frac{b^k - 1}{kb^{k-1}}\,(1 - \chi(p)p^{k-1})\,B_{k,\chi} \neq 0. \tag{25.7}$$

Its valuation V satisfies, with an absolute constant,

$$0 \leq V \leq 1 + C\,np\,\frac{\log(2Np)}{\log p}. \tag{25.8}$$

Proof. Write $X_f = (\mathbb{Z}/f\mathbb{Z})^\times \times \mathbb{Z}_p^\times$, with trivial first group if $f = 1$. For the cylinder of units represented by $1 \leq v \leq fp^m$ at modulus $n_m = fp^m$, assign the value

$$\mu_m(v) = \lfloor bv/n_m \rfloor - (b-1)/2.$$

These p-integral values are compatible under summing over lifts. Indeed for a a power of p the floor sum over $v + un_m$, $0 \leq u < a$, equals $\lfloor bv/n_m \rfloor + (b-1)(a-1)/2$ since multiplication by b permutes residues modulo a. Subtracting the a copies of $(b-1)/2$ gives $\mu_m(v)$. This defines a bounded p-adic integral on X_f. First integrate locally constant functions by finite summation. The absolute value of the result is at most the uniform p-adic norm of the function by the ultrametric inequality, so uniform approximation defines the integral of every continuous function.

For $v \in X_f$, write $u = v^{(p)}/\omega(v^{(p)})$, where $v^{(p)} \in \mathbb{Z}_p^\times$ is its second coordinate. Thus $u \in 1 + p\mathbb{Z}_p$. Form the coefficients

$$c_d = \int_{X_f} \bar{\alpha}'(v)\omega(v^{(p)})^{-h}\frac{(-\log u)^d}{d!}\,d\mu(v).$$

Their asserted valuations follow from $\log u \in p\mathbb{Z}_p$ and boundedness of the integral. Since $v_p(d!) \leq d/(p-1)$, the series converges uniformly on $\mathbb{Z}_p$. Summing the exponential series inside the integral shows that at each integer s its integrand is $\bar{\alpha}'(v)\omega(v^{(p)})^{-h}u^{-s}$. This is odd in v, since $\alpha'(-1) = (-1)^{h-1}$ and u is unchanged by negation. After reduction modulo p^m the integrand is constant on the indicated cylinders, and subtracting the constant $(b-1)/2$ has zero effect modulo p^m by pairing v with $-v$. At $s = r+1$ the integrand is the inverse of $\alpha(v)v^{r+1}$ on units. Consequently the resulting floor sum is (24.4), with prime-to-p conductor f. The proof of Corollary 24.7 applies to the present field by Theorem 24.6. This proves annihilation at every level.

At $s = -j$ the integrand becomes $\chi(v)v^j$ on integer representatives, since $j \equiv -h \bmod (p-1)$. We compute the limit of the uncorrected floor sums against this polynomial, which are congruent to the integral modulo p^m at level m. For units $v \bmod n_m$ put $q_v = \lfloor bv/n_m \rfloor$ and $w = bv - n_m q_v$. The w's permute the units and $\chi(b) = 1$ because $b \equiv 1 \bmod f$. The binomial expansion, summed against $\chi(v)$, gives

$$kb^{k-1}\sum_v \chi(v)v^{k-1}q_v = (b^k - 1)\frac{1}{n_m}\sum_v \chi(v)v^k + O(p^m).$$

Here the error belongs to $p^m O$, since the terms of degree at least two in $n_m q_v$ are divisible by n_m^2 before division by n_m. The integer k is fixed as m tends to infinity.

To compute the normalized moment, first allow all residues, extending χ by zero at nonunits of f. For a residue $a \bmod f$ represented by $1 \leq a \leq f$, sum the powers of $a + fl$, $0 \leq l < p^m$, using

$$\sum_{l=0}^{M-1}(l+z)^k = \frac{B_{k+1}(z+M) - B_{k+1}(z)}{k+1}.$$

This identity follows from the difference formula for Bernoulli polynomials. After division by $M = p^m$ the right side tends p-adically to $B_k(z)$ by the derivative formula. Summing over a and dividing by the remaining f shows that the moment tends to $B_{k,\chi}$. Subtracting the terms divisible by p subtracts $\chi(p)p^{k-1}$ times the all-residue moment at the preceding level. This proves (25.7).

The primitive character χ has parity $(-1)^k$. The identity $B_{k,\chi} = -kL(1-k,\chi)$, proved in Section 25.2 by Mellin integration, and the functional equation show this is nonzero. Indeed the gamma factor at $1-k$ is regular for this parity and the Euler product at $k \geq 2$ is nonzero. The Euler factor in (25.7) is a p-adic unit. Since $p \nmid f$, the p-adic logarithm or the binomial expansion gives $v_p(b^k - 1) = 1 + v_p(k)$. Hence $V = 1 + v_p(B_{k,\chi})$.

For completeness $f(k+1)!\,B_{k,\chi}$ is an algebraic integer. Indeed $(a+1)!B_a \in \mathbb{Z}$ follows inductively from the Bernoulli recurrence. Expanding $B_k(z)$ in the numbers B_a introduces at most one further denominator f in $f^{k-1}B_k(v/f)$. For $0 \leq z \leq 1$ the generating function $we^{zw}/(e^w - 1)$ is uniformly bounded on $|w| = 1$, so $|B_k(z)| \leq C_1 k!$. The absolute value of every conjugate of the cleared integer is thus at most $\exp(C_2 k \log(2fk))$. The field of its character values has degree at most n, as the order of α' divides the exponent of $\mathrm{Gal}(E/\mathbb{Q})$. Taking the absolute rational norm bounds its valuation at any prime above p, normalized by $v_p(p) = 1$, by $C_2 nk \log(2fk)/\log p$. Clearing denominators can only increase that valuation. The inequalities $f \leq N$ and $k \leq p$ prove (25.8). □

Theorem 25.10 (A bound for the number of twists of large exponent)**.** *Let $t \geq 2$ be an integer. Put $D = 2(V+1)$ and $L = V + D\lfloor \log_p t \rfloor$. Among $1 \leq r < t$ in the chosen residue class there are at most D for which $p^L S_{\alpha,r} \neq 0$.*

Proof. Whenever $v_p(\mathcal{A}(r+1)) \leq L$, Theorem 25.9 at precision p^{L+1} rules out an element of order p^{L+1}, by applying its scalar annihilator on that torsion. Any element of greater order would yield one of exactly that order by taking a multiple. Thus a twist counted in the assertion must have $v_p(\mathcal{A}(r+1)) > L$, allowing a zero value to have infinite valuation.

Suppose there are $D+1$ such arguments $s_0, \ldots, s_D$ in $[2,t]$. Let $Q(X) = \prod_i (X - s_i)$. For every d, the remainder $R_d(X)$ of X^d modulo this monic polynomial has integral coefficients and degree at most D. The series $\sum_d c_d R_d(X)$ converges coefficientwise to a polynomial R of degree at most D, and $R(s_i) = \mathcal{A}(s_i)$. For $d \leq D$ the remainder is just X^d, and for $d > D$ the coefficient bound of Theorem 25.9 gives $v_p(c_d) \geq d/2 > V$. Evaluating the integral remainders at $-j$ shows that $R(-j) - \mathcal{A}(-j) \in p^{V+1}O$. In particular $v_p(R(-j)) = V$.

On the other hand evaluate the Lagrange interpolation formula for R at $-j$. In the term with node s_i the numerator of the basis polynomial is integral, and its denominator has valuation at most $D\lfloor \log_p t \rfloor$ since $0 < |s_i - s_l| < t$ for every $l \neq i$. Each term thus has valuation strictly greater than V, as does their sum. This contradiction proves the theorem. □

25.5 An annihilator at primes dividing the field degree

Let $E/\mathbb{Q}$ be finite abelian of degree n and conductor dividing N. Fix any odd prime p. Write $\mathrm{Gal}(E/\mathbb{Q}) = P \times H$, where P is the p-Sylow subgroup. Put $K = E^H$, $d = |P|$, and choose an unramified coefficient ring O over $\mathbb{Z}_p$ containing the values of every character of H. As in Lemma 24.8, extend a character α of H trivially on P, and write $S_\alpha(K)$ for the strict group over K with divisible coefficient $D = (\mathrm{Frac}(O)/O)(\vartheta)$, where $\vartheta = \kappa_p^{-r}\alpha^{-1}$. Here $r \geq 1$ and $\alpha(-1) = (-1)^r$. The prime-to-p order of α gives $\alpha = \alpha'\omega^i$ as in Section 25.4. We use $\overline{\alpha'}$ for the inverse of this finite character and $\bar{\vartheta}$ for the residue-field reduction of ϑ.

Lemma 25.11 (The two kernels in reflection)**.** *Use the determinant $B_{b,m}$ of (24.5). For every $m \geq 1$ and every permissible b,*

$$p^{2w_r} B_{b,m}\, S_\alpha(K)[p^m] = 0, \qquad w_r = \begin{cases} 0, & \bar{\vartheta}|_{G_K} \neq 1, \\ 1 + v_p(d) + v_p(r), & \bar{\vartheta}|_{G_K} = 1. \end{cases}$$

Proof. Choose $\tau \in G_K$ such that $v_p(\vartheta(\tau) - 1) = w_r$. In the first case this is the definition of a nontrivial residual character. In the second, $\bar{\vartheta}$ factors through the p-group P, so its image in the multiplicative group of the residue field is trivial. The prime-to-p characters α and ω^{-r} then have the same reduction and are equal. Choose $g \in G_{\mathbb{Q}}$ with $\kappa_p(g) = 1 + p$ and take $\tau = g^d$. It fixes K, and $\vartheta(\tau) = (1 + p)^{-dr}$ has the required difference from 1 by the p-adic logarithm for odd p.

Take a class $s \in S_\alpha(K)[p^m]$. The coefficient exact sequence for multiplication by p^m lifts s to some $z \in H^1(K, D[p^m])$. Over the cyclotomic field L_m of Section 24.4 the finite coefficient is trivial. Choose a generator of μ_{p^m}. Kummer theory turns the restriction of z into a Kummer class of character $\beta_m = \kappa_{p,m}\vartheta^{-1}$ on $\Gamma_m = \mathrm{Gal}(L_m/K)$, with coefficients extended to $O/p^m O$. Indeed conjugation of the values contributes $\kappa_{p,m}$ and conjugation of the argument contributes ϑ^{-1}.

All its finite valuations are divisible by p^m. On inertia away from p over L_m the original strict class is a coboundary and its divisible coefficient is trivial there. Thus the restricted finite cocycle vanishes on this inertia. A p^m-th root over the maximal unramified extension then has integral valuation in the same value group. At $w \mid p$ the finite cocycle over $L_{m,w}$, viewed in D, is $(\kappa_p^{-r} - 1)y_w$ for a local $y_w \in D$. It factors through the cyclotomic image. Lemma 24.5 supplies unit representatives in every coefficient coordinate. These arguments use the divisible local conditions on s and hold for any choice of its finite lift.

Divide the principal ideal of the Kummer representative by the exponent, sending $(a) = \mathfrak{a}^{p^m}$ to the ideal class of $\mathfrak{a}$. The resulting class is in the β_m-eigenspace. The scalar $B_{b,m}$ kills that ideal class. Indeed the integral Stickelberger element kills the entire class group of L_m. The determinant of its multiplication on the free group algebra over the subgroup Γ_m is a multiple of that element by Cayley–Hamilton. Evaluation on Γ_m at β_m gives $B_{b,m}$ by the coset-basis computation of Theorem 24.9. This calculation applies directly to the image of our class.

The Kummer class of $B_{b,m}z$ over L_m now comes from units and still has character β_m. This character is odd, and K is totally real, since d is odd. The odd part of the unit quotient is generated by roots of unity. In fact complex conjugation c lies in Γ_m, and $u/c(u)$ is a root of unity for every unit of the CM cyclotomic field. Multiplication by two is invertible on the quotient in question. On its roots of unity τ acts as $\kappa_{p,m}(\tau)$. Subtracting the two actions shows that $\vartheta(\tau) - 1$ kills this Kummer class. The assertion includes the case where the odd part is zero.

It follows that $(\vartheta(\tau) - 1)B_{b,m}z$ is in the kernel of restriction to L_m. By inflation–restriction this kernel comes from $H^1(\Gamma_m, D[p^m])$. If y is a cocycle on this abelian group, commuting $\tau|_{L_m}$ with σ in its cocycle identity gives

$$(\vartheta(\tau) - 1)y(\sigma) = (\vartheta(\sigma) - 1)y(\tau|_{L_m}).$$

The right side is a coboundary. Thus $(\vartheta(\tau) - 1)^2 B_{b,m}$ kills z, hence its image s. The square has valuation $2w_r$. □

Fix r mod $(p-1)$, put $h = r+1+i$ mod $(p-1)$, and let $j \in [1, p-1]$ satisfy $j \equiv -h$ mod $(p-1)$. Write $k = j + 1$. Let A be the least common multiple of the conductors of K and α, $F =$

$A/p^{v_p(A)}$, $a = \max(1, v_p(A))$, and $M = Fp^a$. In particular $M \le pN$. We use $b = 1 + M$. For a character ξ on the units modulo M, set

$$B_{k,\xi;M} = M^{k-1} \sum_{\substack{1 \le v \le M \\ (v,M)=1}} \xi(v) B_k(v/M).$$

Theorem 25.12 (A determinant varying with the twist)**.** *There is a series $\mathcal{B}(X) = \sum_{l \ge 0} b_l X^l$ over O with $v_p(b_l) \ge l - v_p(l!)$. For every positive twist in the fixed class and every $m \ge 1$, $p^{2w_r}\mathcal{B}(r+1)$ annihilates $S_\alpha(K)[p^m]$. Its value at $-j$ is nonzero and equals*

$$\mathcal{B}(-j) = \left(\frac{b^k - 1}{k b^{k-1}}\right)^d \prod_{\eta \in \widehat{P}} B_{k,\overline{\alpha'}\eta^{-1};M}. \tag{25.9}$$

Here η is viewed as the Dirichlet character of K through the cyclotomic quotient. The product is evaluated in a splitting field for P.

Proof. On $(\mathbb{Z}/F\mathbb{Z})^\times \times \mathbb{Z}_p^\times$, take the measure whose value on the cylinder $v \bmod Fp^m$ is $\lfloor bv/(Fp^m) \rfloor - (b-1)/2$, with its least positive representative. Compatibility and boundedness follow from the floor identity in the proof of Theorem 25.9. Denote by $\sigma(v)|_K$ the image in P of the unit residue of v modulo M acting on roots of unity. Write $v^{(p)}$ for the second coordinate of v and $\langle v \rangle = v^{(p)}/\omega(v^{(p)})$. With values in $O[P]$, integrate the series

$$\overline{\alpha'}(v)\, \omega(v^{(p)})^{-h} [\sigma(v)^{-1}|_K]\, \exp(-X \log\langle v \rangle)$$

coefficient by coefficient against the measure. Call the result $U(X)$. Every coordinate of its l-th coefficient has valuation at least $l - v_p(l!)$ by boundedness of the measure. Let $\mathcal{B}(X)$ be the determinant of multiplication by $U(X)$ on the basis P. For degrees $l_1 + \cdots + l_d = l$, $\sum_i v_p(l_i!) \le v_p(l!)$ by the integral multinomial coefficient. The determinant expansion gives the stated bound and uniform convergence on $\mathbb{Z}_p$.

The integrand is odd in v, since its scalar weight is odd and complex conjugation acts trivially on K. The constant correction to the floors therefore cancels. For $m \ge a$ the modulus n_m of (24.5) equals Fp^m. At $X = r+1$ the integrand modulo p^m is constant on these cylinders, and its determinant after integration is exactly $B_{b,m}$. Lemma 25.11 gives the asserted annihilator. For $m < a$ the same conclusion follows by including the p^m-torsion in the p^a-torsion.

Over a characteristic-zero splitting field the regular representation of the abelian group P splits into its individual characters. At $X = -j$ evaluation on η turns the integrand on integer representatives into $\xi(v) v^{k-1}$, where $\xi = \overline{\alpha'}\eta^{-1}$ on units modulo M. At $n_m = Mp^{m-a}$, multiplication by b permutes the units and fixes ξ, since $b \equiv 1 \bmod M$. The binomial calculation in the proof of Theorem 25.9 gives the integral as $(b^k - 1)/(kb^{k-1})$ times the limit of $n_m^{-1} \sum_v \xi(v) v^k$ over unit residues. Splitting this sum into progressions $v = u + Ml$ with u a unit modulo M and applying the Bernoulli difference formula as in that proof gives exactly $B_{k,\xi;M}$. Multiplication over η proves the formula.

To verify nonvanishing, let ξ_0 be the primitive character inducing ξ, of conductor $g \mid M$. The Bernoulli distribution formula gives

$$B_{k,\xi;M} = B_{k,\xi_0} \prod_{\substack{q \mid M,\ q \text{ prime} \\ q \nmid g}} (1 - \xi_0(q) q^{k-1}).$$

Indeed, the sum with the primitive weight extended by zero at nonunits of g, before imposing the extra coprimality conditions, has the same normalized value for every multiple of g. This

follows by grouping the terms above each residue modulo g and using $\sum_{l=0}^{D-1} B_k((z+l)/D) = D^{1-k}B_k(z)$. Deleting multiples of a squarefree divisor u of the extra primes contributes $\xi_0(u)u^{k-1}$ times that value in inclusion–exclusion. This proves the product formula. Every Euler factor is nonzero since $k \geq 2$, and $\xi_0(-1) = (-1)^k$ since η is even. The primitive functional equation at $1-k$ and the Euler product at k give $B_{k,\xi_0} \neq 0$ as in Theorem 25.9. □

Corollary 25.13 (Counting twists at every odd prime)**.** *Fix an integer $t \geq 2$. For the fixed α, h put $V_{\alpha,h} = v_p(\mathcal{B}(-j))$ and $D_0 = 2(V_{\alpha,h}+1)$. All but at most D_0 of the twists $1 \leq r < t$ in the chosen class satisfy*

$$p^{V_{\alpha,h}+D_0\lfloor \log_p t\rfloor + 2w_r} S_\alpha(K) = 0.$$

For each rational conjugacy orbit $\mathcal{O}$ of characters of H and each h with the required parity,

$$\sum_{\alpha\in\mathcal{O}} (1+V_{\alpha,h}) \ll |\mathcal{O}|\, d\, k\, \frac{\log(2Np)}{\log p}. \tag{25.10}$$

The implicit constant is absolute.

Proof. The interpolation proof of Theorem 25.10 uses only the bound $v_p(b_l) \geq l/2$, the distinct integral arguments in $[2,t]$, and the nonzero value at $-j$ in the unramified ring O. It bounds the number of arguments with valuation larger than $V_{\alpha,h} + D_0\lfloor \log_p t\rfloor$ by D_0. At each other argument Lemma 25.11 and Theorem 25.12 supply the displayed exponent. Indeed an element of larger order would have a multiple of order exactly one power higher, where the finite-level annihilator already applies.

For the orbit estimate k is fixed by h, and M is constant on the orbit. Each $M(k+1)!B_{k,\xi;M}$ is an algebraic integer of absolute value at most $\exp(Ck\log(2Mk))$ at every embedding, by the Bernoulli polynomial expansion and the estimate on $[0,1]$ in Theorem 25.9. The product of these integers over $\widehat{P}$ lies in the value field of α. Indeed its prime-to-p factor α' takes values there and every automorphism fixing that field permutes the factors indexed by η. Embeddings of the value field correspond to $\mathcal{O}$. Take the absolute rational norm of the product. The sum of its valuations over those embeddings is at most $C|\mathcal{O}|dk\log(2Mk)/\log p$. The cleared integer denominators can only increase that sum. Finally $v_p((b^k-1)/(kb^{k-1})) = a$ by $v_p(b-1) = a$ and the logarithm. Adding $|\mathcal{O}|(1+da)$, using $p^a \leq M \leq pN$ and $k \leq p$, proves (25.10). □

25.6 Bernoulli units at large two-power conductor

Fix an odd prime p and an embedding of the algebraic character values in $\overline{\mathbb{Q}}_p$. Let $Q = p^D$ with $D \geq 1$ and $Q \equiv 1 \bmod 4$, and put $e = v_2(Q-1)$. Let ϕ be a primitive Dirichlet character of odd conductor f and order dividing $Q-1$. Let ξ be primitive of conductor $M = 2^s$. We extend characters by zero on nonunits, and suppose $\phi(-1)\xi(-1) = -1$. Thus $\phi\xi$ is a nontrivial odd character of conductor fM. The following estimate is uniform at the primes above p, including when $p \mid f$.

Theorem 25.14 (A unit criterion in the two-power tower)**.** *If $M \geq f4^e$, then*

$$B_{1,\phi\xi} = \frac{1}{fM}\sum_{a=0}^{fM-1} a\phi(a)\xi(a) \quad \textit{is a } p\textit{-adic unit.}$$

The conclusion also holds with both characters replaced by their inverses.

Proof. First group the integers in the sum by their class u mod M. Set

$$A(u) = \frac{1}{fM}\sum_{\substack{0\leq a<fM\\ a\equiv u\ (M)}} a\phi(a), \qquad G(u) = A(u) - A(0), \qquad S = \sum_{a \bmod f} \phi(a).$$

The unweighted sum of $\phi(a)$ in each such class is S, since M is prime to f. Write $[u] \in [0, M-1]$ for the representative of u. For a multiple $b = ft \leq M$, shifting representatives by b gives

$$G(u) - G(u-b) = \frac{tS}{M} - \mathbf{1}_{[u]<b}\phi([u]). \tag{25.11}$$

Indeed the shift preserves ϕ, adds b to each representative, and subtracts fM exactly for representatives which end in $[0, b-1]$. This interval contains at most one integer in the given class. Starting at $G(0) = 0$ and using the shift f, one obtains every $G(u)$, since f generates the additive group modulo M. Formula (25.11) therefore makes all $G(u)$ integral at p, even when f is divisible by p. Their reductions lie in $\mathbf{F}_Q$, since the nonzero values of ϕ are $(Q-1)$-st roots of unity. We have $B_{1,\phi\xi} = \sum_u \xi(u)G(u)$, since $\sum_u \xi(u) = 0$. This also proves its integrality.

Work now in a finite residue field containing $\mathbf{F}_Q$ and all M-th roots of unity. Write the reduced G, ϕ, ξ with the same letters. Put $m = s - e$, so $m \geq e \geq 2$, and

$$C = \{u \in (\mathbb{Z}/M\mathbb{Z})^\times : \xi(u)^{2^e} = 1\}.$$

Suppose the Bernoulli sum is zero in this field. For every unit $y \bmod M$, changing u to uy gives $\sum_u \xi(u)G(uy) = 0$. This forces

$$\sum_{u \in C} \xi(u)G(uy) = 0 \qquad \text{for every unit } y. \tag{25.12}$$

To see this, average the equations obtained by applying the first 2^m powers of the Q-power Frobenius. They fix all $G(uy)$. The powers of Q modulo M run through exactly the residues $1 + 2^e j$, $0 \leq j < 2^m$. Indeed $v_2(Q^{2^a} - 1) = e + a$ by repeated squaring, since $Q \equiv 1 \bmod 4$. This gives order 2^m in the subgroup of that size. For $z = \xi(u)$ the average is z times the average of the powers of z^{2^e}. The geometric sum is zero unless $z^{2^e} = 1$. Division by 2^m is permitted in odd characteristic. This proves (25.12).

Every $u \in C$ satisfies $u \equiv 1$ or $-1 \bmod 2^m$. In fact the units modulo 2^s are $\{\pm 1\} \times \langle 5 \rangle$. The equality $v_2(5^{2^a} - 1) = 2 + a$ proves that 5 generates the subgroup congruent to 1 mod 4. Primitivity of ξ means that it takes the value -1 on $1 + M/2$, the nonidentity element of the kernel of reduction to $M/2$. Thus $\xi(5)$ has order 2^{s-2}, also after reduction at p. Writing $u = \pm 5^a$, the condition on $\xi(u)$ forces $2^{m-2} \mid a$, as asserted. The two signs are distinct since $m \geq 2$.

Take $b = f2^e$, so $1 < b \leq 2^m$, and subtract (25.12) at $y = 1 - b$ from the same equation at $y = 1$. For the sign $+$ one has $u(1-b) = u - b \bmod M$, since $2^m \mid u - 1$ and $2^e \mid b$. In (25.11) the indicator is nonzero only at $u = 1$, where $\xi(1)\phi(1) = 1$. For the sign $-$ one has $u(1-b) = u + b$. Use (25.11) at $u + b$ with the opposite sign. Its indicator is nonzero only if $[u + b] = b - 1$, equivalently $u = -1$. This time its signed contribution is $\xi(-1)\phi(b-1) = \xi(-1)\phi(-1) = -1$. The constant terms have total zero. Indeed multiplication by $1 + M/2$ permutes each sign in C and negates $\xi(u)$. The difference of the two zero sums is therefore $-1 - 1$, a contradiction in characteristic p. The inverse characters satisfy the same hypotheses. □

Corollary 25.15 (Residual cocycles unramified after restriction)**.** *Let γ be the reduction of $\phi\xi$ in a finite field k of characteristic p, with the hypotheses of Theorem 25.14. Let $\delta = \gamma$ or γ^{-1}. Suppose a continuous cocycle $z : G_{\mathbb{Q}} \to k(\delta)$ vanishes on a subgroup of finite index prime to p in $I_v \cap \ker \delta$ for every finite inertia group I_v. Then z is a coboundary.*

Proof. The restriction to $I_v \cap \ker \delta$ is an additive homomorphism. The index of its kernel divides the stipulated index, while its image is a finite p-group. Thus it vanishes on all of $I_v \cap \ker \delta$. Over $L = \mathbb{Q}(\zeta_{fM})$ the restriction of z is an everywhere unramified additive homomorphism,

and L has no real places. Class field theory identifies it with a homomorphism $u : \mathrm{Cl}(\mathcal{O}_L) \to k$. The cocycle identity gives $u(\sigma c) = \delta(\sigma)u(c)$ for every ideal class c and $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, using the Galois action on classes under reciprocity.

Choose a positive integer $b \equiv 1 \bmod \mathrm{lcm}(p, f)$ and $b \equiv 1 + M/2 \bmod M$ by the Chinese remainder theorem. The integral Stickelberger element $(b-\sigma_b)\Theta_{fM}$ annihilates the class group by Stickelberger's theorem, used in Section 24.2. Let δ_0 be the corresponding character in characteristic zero. Evaluation of the element at δ_0 gives $(b - \delta_0(b))B_{1,\delta_0^{-1}}$ by the defining sum for Θ_{fM}. The first factor reduces to 2 and the second is a unit by Theorem 25.14. The group-ring element thus acts by an invertible scalar on the image of u, forcing $u = 0$. The remaining class inflates from the finite abelian group $\mathrm{Gal}(L/\mathbb{Q})$. Commuting a group element of character -1 with an arbitrary element in the cocycle identity shows that multiplication by -2 is a coboundary on this class. This proves its vanishing. □

The finite Fourier argument above reconstructs `Development/AutomorphicArithmetic/AutomorphicVarieties/LevelCohomology/LemmaX.lean`, line 78. The two translated sums occur in `Development/AutomorphicArithmetic/AutomorphicVarieties/LevelCohomology/LxCore.lean`, line 139. The application to residual cocycles appears in `Development/AutomorphicArithmetic/AutomorphicVarieties/LevelCohomology/ChrInvNeg.lean`, line 197.

25.7 Effective descent in the real cyclotomic tower

Let $E/\mathbb{Q}$ be finite abelian. Use the notation of Section 25.5 at an odd prime p, so that $\mathrm{Gal}(E/\mathbb{Q}) = P \times H$, $K = E^H$, and α is a character of H extended trivially on P. Choose $r \geq 1$ with $\alpha(-1) = (-1)^r$. Let $\beta = \omega^{r+1}\alpha$ denote the characteristic-zero Teichmüller character of the residual reflected action. It is odd. Let $M_1 = \mathrm{lcm}(p, \mathrm{cond}\, K, \mathrm{cond}\, \alpha)$, and factor the primitive character inducing β as $\phi\xi$ of conductor $f2^s$ with f odd and ξ of two-power conductor 2^s.

Proposition 25.16 (A vanishing test including primes dividing the degree)**.** *Suppose $D \geq 1$, $Q = p^D \equiv 1 \bmod 4$, the order of ϕ divides $Q - 1$, and $2^s \geq f4^e$ with $e = v_2(Q - 1)$. Suppose also that each prime $q \mid M_1$ not dividing $f2^s$ satisfies $q \not\equiv \pm 1 \bmod 2^{s-e}$. Then $S_\alpha(K) = 0$.*

Proof. The primitive value $B_{1,\beta^{-1}}$ is a p-adic unit by Theorem 25.14. On enlarging the modulus to M_1 the Bernoulli number becomes

$$B_{1,\beta^{-1};M_1} = B_{1,\beta^{-1}} \prod_{\substack{q \mid M_1,\ q \text{ prime} \\ q \nmid f2^s}} (1 - \beta^{-1}(q)).$$

This follows by the Bernoulli distribution formula and inclusion–exclusion as in Theorem 25.12, now at $k = 1$. If any extra factor vanishes modulo p, then $\xi(q) \bmod p$ is in $\mathbf{F}_Q^\times$. Its order is a power of two dividing 2^e. The description of C in the proof of Theorem 25.14 would give $q \equiv \pm 1 \bmod 2^{s-e}$. Thus every factor is a unit.

The first-level residual character $\bar{\vartheta}$ on G_K is nontrivial. Indeed on $G_\mathbb{Q}$ it is the reduction of $\omega\beta^{-1}$, whose two-power conductor is 2^s. If it were trivial on G_K it would factor through the p-group $\mathrm{Gal}(K/\mathbb{Q})$, which has no nontrivial character in the multiplicative residue field. Choose $b \equiv 1 \bmod (M_1)_{\mathrm{odd}}$ and $b \equiv 1 + 2^{s-1} \bmod 2^s$, where $(M_1)_{\mathrm{odd}}$ denotes the odd part of M_1. This makes b prime to M_1, $\beta(b) = -1$, and $b \equiv 1 \bmod p$.

The augmentation of the group-algebra element in (24.5) at $m = 1$ is the reduction of

$$\sum_{v \in (\mathbb{Z}/M_1\mathbb{Z})^\times} \lfloor b[v]/M_1 \rfloor\, \beta^{-1}(v) = (b - \beta(b))B_{1,\beta^{-1};M_1}.$$

Here $[v]$ is its least positive representative. To obtain the equality, permute representatives by $v \mapsto bv$ and use $[bv] = b[v] - M_1\lfloor b[v]/M_1 \rfloor$. The constant term in $B_1(z) = z - 1/2$ sums to zero against the odd character. The augmentation is therefore nonzero. Over the residue field the determinant of multiplication on its group algebra of P is the $|P|$-th power of that augmentation, by the nilpotence calculation in Theorem 24.9. It kills $S_\alpha(K)[p]$ by that theorem and is a unit. Any nonzero element in the p-primary group would have a multiple of order p, so the entire group vanishes. □

Fix a primitive character ψ of conductor F, let $o = [K_\psi : \mathbb{Q}]$, and put $B_j = K_\psi C_j$ with $C_j = \mathbb{Q}(\zeta_{2^{j+2}})^+$. For B_j or any other abelian field write $M_{p,r} = \frac{1}{2}(1 + (-1)^r c)\mathcal{S}_{p,r}$. Let $D = 2\varphi(o)$, where $\varphi(1) = 1$. For every odd prime p put

$$e_p = v_2(p^D - 1), \qquad H_p = 4(F+2)(p+1)4^{e_p}, \qquad a_p = \min\{a \geq 0 : 2^{a+2} \geq H_p\}. \tag{25.13}$$

Theorem 25.17 (An explicit layer for every complementary twist)**.** *For every odd prime p, every $r \geq 1$, and every $J \geq a_p$, restriction gives an isomorphism*

$$M_{p,r}(B_{a_p}) \;\simeq\; M_{p,r}(B_J).$$

For $J < a_p$ it gives an injection in the other direction. The field B_{a_p} has degree and cyclotomic modulus $O_\psi((p+1)4^{e_p}) = O_\psi(p^3)$.

Proof. Write a character α of the prime-to-p part of $\mathrm{Gal}(B_J/\mathbb{Q})$ as $\lambda\zeta$, where λ comes from K_ψ and ζ from C_J. Such a factorization holds because the restriction map embeds the Galois group of the compositum in the product of the two Galois groups, and a finite abelian subgroup character extends to the product. To extend across one generator whose coset has order a, choose an a-th root of the prescribed value on its a-th power. Repeating this proves the claim. Choose all values as algebraic roots of unity. Since ζ has two-power order and α has order prime to p, the pullback of λ to the compositum has order prime to p. The restriction to K_ψ is onto, so the order of λ divides the prime-to-p part of o.

Let 2^s be the two-part of the conductor of α. In $\beta = \omega^{r+1}\alpha = \phi\xi$ the dyadic character has the same conductor, since p is odd. The odd conductor f of ϕ divides pF, and its order divides $\mathrm{lcm}(p-1, o/p^{v_p(o)})$. For any divisor u of o, $\varphi(u)$ divides $\varphi(o)$, as seen prime by prime in the formula for Euler's totient. Thus $p^D \equiv 1 \bmod o/p^{v_p(o)}$, and D also ensures $p^D \equiv 1 \bmod 4$. The order condition in Proposition 25.16 follows.

The p-power subfield K of B_J is contained in K_ψ, since $[B_J : K_\psi]$ is a power of two. The odd prime divisors of M_1 are consequently among the primes dividing pF. If $2^s > H_p$, then $2^s > f4^{e_p}$ and $2^{s-e_p} > \max(p, F) + 1$. Each odd prime in M_1 outside the primitive conductor lies strictly between 1 and $2^{s-e_p} - 1$. Proposition 25.16 eliminates this component through every exponent.

It remains to interpret the components with $2^s \leq H_p$. The dyadic conductor of λ divides $2^{v_2(F)}$, and that of $\zeta = \alpha/\lambda$ divides the larger of $2^s, 2^{v_2(F)}$, hence divides 2^{a_p+2}. As an even character of two-power conductor, ζ factors through C_{a_p}. Therefore α is trivial on $\mathrm{Gal}(B_J/B_{a_p})$ when $J \geq a_p$. Over unramified coefficients the integral idempotents for the prime-to-p part now show that the whole complementary group is invariant under this two-group, including its components with nontrivial P-action. Descent for a prime-to-p extension identifies those invariants with the strict group downstairs, since averaging gives exact invariants globally and on each inertia and decomposition group. This argument respects complex conjugation, and faithful scalar extension gives the claimed integral result. If $J < a_p$ restriction followed by corestriction is multiplication by the two-power relative degree, so restriction is injective.

Finally

$$e_p = v_2(p-1) + v_2(p+1) + v_2(D) - 1 = \max(v_2(p-1), v_2(p+1)) + v_2(D).$$

For the first equality use $v_2(p^u - 1) = v_2(p-1)$ for odd u and repeated squaring after the first factorization of $p^{2u} - 1$. Precisely one of $p-1, p+1$ has valuation one, which gives the second equality. Thus $2^{e_p} \le 2^{v_2(D)}(p+1)$. Both the degree and the modulus are at most $F 2^{a_p+2} \le 2FH_p$, which gives the bounds. □

25.8 Bernoulli values shared by different coefficient primes

Fix a finite abelian extension $E/\mathbb{Q}$ of degree n in $\mathbb{Q}(\zeta_N)$. Let c denote complex conjugation. For an odd prime p and a positive integer r, put

$$M_{p,r}(E) = \tfrac{1}{2}(1 + (-1)^r c) \ker\left[H^1(\mathcal{O}_E[1/p], (\mathbb{Q}_p/\mathbb{Z}_p)(-r)) \longrightarrow \prod_{w \mid p} H^1(E_w, (\mathbb{Q}_p/\mathbb{Z}_p)(-r)) \right].$$

We use continuous Galois cohomology, unramified away from p in the global term. Suppose first that $p \nmid nN$. Fix an embedding of the algebraic character values into $\overline{\mathbb{Q}}_p$. Take O to be the ring of integers of a finite unramified extension of $\mathbb{Q}_p$ containing the values of all characters of $G = \mathrm{Gal}(E/\mathbb{Q})$. Such an extension exists since $p \nmid n$. Normalize $v_p(p) = 1$. A character of G will be written as its primitive Dirichlet character. For $\alpha(c) = (-1)^r$, let $S_{\alpha,r}$ denote the α-component of $M_{p,r}(E) \otimes O$. The idempotents for G are integral at p. Their sum over this parity is the identity on the indicated module.

Write $\chi = \bar{\alpha} = \alpha^{-1}$ on the units of its conductor f. Let $k \ge 2$ with $k + r \equiv 0 \bmod (p-1)$. Then χ has parity $(-1)^k$. With the convention $B_1 = -1/2$, put

$$z_{k,\chi} = \frac{B_{k,\chi}}{k}, \qquad B_{k,\chi} = f^{k-1} \sum_{a=1}^{f} \chi(a) B_k(a/f).$$

For the trivial character take $f = 1$. The identity $z_{k,\chi} = -L(1-k, \chi)$ and the functional equation give $z_{k,\chi} \neq 0$. Indeed the archimedean gamma factors at $1-k$ and k are regular for this parity, and the Euler product at $k > 1$ is nonzero.

Lemma 25.18 (Comparison at a negative integer)**.** *If $\alpha = 1$ and $p - 1 \mid r$, then $S_{\alpha,r} = 0$. In every other case $v = v_p(z_{k,\chi})$ is a nonnegative integer. If $v < 1 + v_p(r+k)$, then $p^v S_{\alpha,r} = 0$. In particular $v = 0$ gives vanishing for every positive twist in the residue class $-k \bmod (p-1)$.*

Proof. Let ω be the Teichmüller character at p. As in Theorem 24.6, character descent gives the coefficient character $\alpha^{-1}\kappa_p^{-r}$ over $\mathbb{Q}$, where κ_p is the cyclotomic character. Its residual character on $(\mathbb{Z}/f\mathbb{Z})^\times \times \mathbf{F}_p^\times$ is $\chi\,\omega^k \bmod p$. Triviality is equivalent to $\alpha = 1$ and $p - 1 \mid r$, by the independence of the two factors and injectivity of reduction on the roots of unity of order prime to p. Theorem 24.6 gives the first assertion in precisely this case.

Otherwise choose a positive integer $b > 1$, prime to fp, at which $\chi(b) b^k \not\equiv 1 \bmod pO$. Such a residue exists because the residual character is nontrivial, and lifts by the Chinese remainder theorem. Let $X_f = (\mathbb{Z}/f\mathbb{Z})^\times \times \mathbb{Z}_p^\times$. For a unit residue a at modulus $m = fp^l$, represented in $[1, m]$, give its cylinder the weight $\lfloor ba/m \rfloor - (b-1)/2$. These weights define a bounded O-valued measure μ_b. In fact the child residues are $a + mi$ for $0 \le i < p$, and $bi \bmod p$ permutes the residues modulo p. Summing their floors gives $\lfloor ba/m \rfloor + (b-1)(p-1)/2$, proving compatibility for $l \ge 1$. Each weight is integral since p is odd. For the p-coordinate of a, put $\langle a \rangle = a^{(p)}/\omega(a^{(p)})$. With $h = r + 1 \bmod (p-1)$, set

$$A_b(s) = \int_{X_f} \chi(a) \omega(a^{(p)})^{-h} \langle a \rangle^{-s}\, d\mu_b(a) \qquad (s \in \mathbb{Z}_p).$$

The bounded integral is the limit of locally constant approximations. At $s = r+1$ its integrand modulo p^l is $\alpha(a)^{-1}a^{-r-1}$. Its sign at $-a$ is negative. Thus the constant subtracted from the floors contributes zero, by pairing the residues. The finite floor sum annihilates $S_{\alpha,r}[p^l]$ by Corollary 24.7. This is the class-group annihilation from the integral Stickelberger element on the cyclotomic field of conductor fp^l.

At $s = 1-k$ the integrand on integer representatives is $\chi(a)a^{k-1}$. To compute its integral let $q_a = \lfloor ba/m \rfloor$ and $w_a = ba - mq_a$. The w_a permute the units modulo m and $\chi(w_a) = \chi(b)\chi(a)$. Expanding w_a^k, multiplying by $\chi(a)$, and summing over the units gives

$$kb^{k-1}\sum_a \chi(a)a^{k-1}q_a \equiv (b^k - \chi(b)^{-1})\, m^{-1}\sum_a \chi(a)a^k \pmod{p^l O}.$$

Every binomial term of degree at least two in mq_a contains m^2 before division by m. For the normalized sum on the right, first allow multiples of p. On each progression modulo f the identity $\sum_{i=0}^{u-1}(y+i)^k = (B_{k+1}(y+u) - B_{k+1}(y))/(k+1)$ with $u = p^l$ gives the limit $B_{k,\chi}$ after summation and normalization. Indeed the linear term of the numerator is $(k+1)B_k(y)u$ and every higher term tends to zero after division by u. Deleting multiples of p subtracts $\chi(p)p^{k-1}$ times the preceding normalized sum. The integral of the constant correction again vanishes by oddness. Letting l tend to infinity gives

$$A_b(1-k) = (b^k - \chi(b)^{-1})b^{1-k}(1-\chi(p)p^{k-1})\, z_{k,\chi}. \tag{25.14}$$

All factors multiplying $z_{k,\chi}$ are units. Thus its valuation equals the valuation of an integral and is nonnegative. Moreover $\langle a\rangle^{r+k} \equiv 1 \bmod p^{1+v_p(r+k)}$ for every a, by the binomial theorem on $1 + p\mathbb{Z}_p$. Boundedness gives the same congruence between $A_b(r+1)$ and $A_b(1-k)$. Under the strict inequality in the lemma both have valuation v. The annihilator at $l = v+1$ rules out a cyclic summand of order p^{v+1}, hence also an element of any larger order. □

For each $k \geq 2$ take one representative α from each rational conjugacy orbit of characters of G of parity $(-1)^k$. Write $F_\alpha = \mathbb{Q}(\alpha)$ for the field of values. In its ring of integers factor the principal fractional ideal of $z_{k,\bar{\alpha}}$ into a quotient of relatively prime integral ideals. Write $\mathfrak{a}_{k,\alpha}$ for the numerator ideal and define the positive rational integer

$$J_k(E) = \prod_{\alpha \text{ representative}} \mathrm{N}_{F_\alpha/\mathbb{Q}}(\mathfrak{a}_{k,\alpha}). \tag{25.15}$$

An empty product equals one. Ideal norms make this independent of the representatives. In particular the same integer can be used at different coefficient primes.

Theorem 25.19 (An integer for all primes at a fixed weight)**.** *For $k \geq 2$ one has $\log J_k(E) \ll nk\log(2Nk)$ with an absolute constant. For every odd $p \nmid nN$ put $w = v_p(J_k(E))$. If $p-1 \mid r+k$ and $w < 1 + v_p(r+k)$, then*

$$p^w M_{p,r}(E) = 0.$$

In particular $M_{p,r}(E) = 0$ for all positive $r \equiv -k \bmod (p-1)$ at an odd prime $p \nmid nNJ_k(E)$.

Proof. For each prime p, the embeddings of F_α into $\overline{\mathbb{Q}}_p$ over a fixed prime ideal $\mathfrak{p} \mid p$ number $e_\mathfrak{p} f_\mathfrak{p}$, its ramification index times its residue degree. With $v_p(p) = 1$, their total positive valuation on $z = z_{k,\bar{\alpha}}$ is $f_\mathfrak{p}\max(0, \mathrm{ord}_\mathfrak{p}\, z)$. Summing first over $\mathfrak{p}$ and then over the orbits yields

$$v_p(J_k(E)) = \sum_{\alpha(c)=(-1)^k} \max\{0, v_p(z_{k,\bar{\alpha}})\}, \tag{25.16}$$

where every individual character occurs once on the right.

The integer $a = fk(k+1)!$ clears the denominators of z. Indeed $(i+1)!B_i \in \mathbb{Z}$ follows from the Bernoulli recurrence, and in $f^{k-1}B_k(j/f)$ at most one further factor f is needed. The numerator ideal of z divides the integral ideal (az), so its norm is at most $|\mathrm{N}(az)|$. The generating function $ue^{yu}/(e^u-1)$ on $|u|=1$ gives $|B_k(y)| \le Ck!$ uniformly for $0 \le y \le 1$. It follows that every complex conjugate of az has absolute value at most $\exp(C'k\log(2Nk))$. The sum of the degrees of the orbit representatives equals the number of characters of that parity, at most n. Multiplication proves the height bound. Equation (25.16) bounds the nonnegative valuation at each nontrivial residual component by w. Apply Lemma 25.18 to each component and descend the annihilation through the faithfully flat extension to O. □

Theorem 25.20 (Counting exceptional twists across primes)**.** *Let $t \ge 2$ be an integer and $Y \ge 3$ a real number. For each odd $p \le Y$ with $p \nmid nN$ there is a set $\mathcal{E}_p \subseteq \{1,\dots,t-1\}$ such that*

$$\sum_{\substack{2<p\le Y\\ p \text{ prime},\ p\nmid nN}} |\mathcal{E}_p| \log p \;\le\; 2\sum_{k=2}^{\lfloor Y\rfloor} \log J_k(E) \;\ll\; nY^2\log(2NY). \tag{25.17}$$

For $1 \le r < t$ outside $\mathcal{E}_p$, let k be the unique integer in $[2,p]$ congruent to $-r \bmod (p-1)$. Then

$$p^{(1+2\lfloor \log_p t\rfloor)v_p(J_k(E))} M_{p,r}(E) = 0.$$

Here $\log_p t = (\log t)/(\log p)$.

Proof. Fix a nontrivial residual component and its class of $r \bmod (p-1)$. In Lemma 25.18 we may hold b,h,k fixed on that class. Write $v = v_p(z_{k,\chi})$. At $v=0$ every group in the class vanishes. Suppose $v \ge 1$ and put $D = 2v$. In the expansion $A_b(s) = \sum_{i\ge 0} c_i s^i$, bounded integration of $(-\log\langle a\rangle)^i/i!$ gives $v_p(c_i) \ge i - v_p(i!) \ge i/2$. The series converges uniformly on $\mathbb{Z}_p$.

At most D integers $s = r+1$ in the class and in $[2,t]$ can have $v_p(A_b(s)) > v + D\lfloor \log_p t\rfloor$. In fact, if there were $D+1$ distinct such points, reduce each monomial of the series modulo their monic product $\prod_j (X - s_j)$. All remainders are integral, so the sum of the reduced series is a polynomial R of degree at most D. At the nodes it has values $A_b(s_j)$. Terms of index $i > D$ have valuation greater than v, giving $R(1-k) \equiv A_b(1-k) \bmod p^{v+1}$. The latter has valuation v by (25.14). On the other hand, evaluating the Lagrange interpolation formula for R at $1-k$ gives terms of valuation strictly greater than v. Each denominator is a product of D nonzero differences of absolute value less than t, and each numerator factor is integral. This is a contradiction.

Put those exceptional twists into $\mathcal{E}_p$, taking the union over all characters and classes. At every other twist the finite-level annihilator bounds the exponent as in the lemma. The exceptional count for a single character and k is at most $2v$, including when $v=0$. Components trivial residually need no exceptions. Summing (25.16) first at p, and then interchanging the finite sums over p and $2 \le k \le p$, uses each prime factor of $J_k(E)$ at most to its multiplicity. This proves (25.17). The last estimate follows by summing Theorem 25.19 over $k \le Y$. □

Corollary 25.21 (Vanishing in shifted residue classes)**.** *For every odd prime p and every positive even r,*

$$K_{2r}(\mathbb{Z})\{p\} = 0 \quad \text{if } p-1 \mid r+k \text{ for some } k \in \{2,4,6,8,10,14\}.$$

In particular $K_{2p-6}(\mathbb{Z})\{p\} = 0$ for every prime $p \ge 5$. For $E = \mathbb{Q}(i)$ the entire group $M_{p,r}(E)$ vanishes for every odd prime p and every positive odd r with $p-1 \mid r+3$.

Proof. Over $\mathbb{Q}$ the Bernoulli recurrence gives, in order of increasing k,

$$\frac{1}{12},\quad -\frac{1}{120},\quad \frac{1}{252},\quad -\frac{1}{240},\quad \frac{1}{132},\quad \frac{1}{12}$$

for B_k/k. Thus their numerator ideals all have norm one. Theorem 25.19 gives the vanishing of $M_{p,r}(\mathbb{Q})$. For even r, its Pontryagin dual is $K_{2r}(\mathbb{Z})\{p\}$. Indeed the localization sequence and odd-primary Quillen–Lichtenbaum comparison identify the latter with $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(r+1))$, and Poitou–Tate identifies the dual of the kernel of localization there with the strict group. The local H^2 term is dual to $H^0(\mathbb{Q}_p, (\mathbb{Q}_p/\mathbb{Z}_p)(-r))$. Global and local cyclotomic images are both $\mathbb{Z}_p^\times$, so their invariants agree. Exactness of the final localization and sum-of-invariants maps therefore makes all the global H^2 strict. These identifications are given in Section 25.2 and in the proof of Corollary 11.18. For $E = \mathbb{Q}(i)$ only χ_{-4} has odd parity. Since $B_3(u) = u^3 - 3u^2/2 + u/2$, one has $4^2(B_3(1/4) - B_3(3/4))/3 = 1/2$. Thus $J_3(E) = 1$. Taking $N = 4$ gives $nN = 8$, prime to every odd p. □

25.9 Character comparison at primes dividing the degree

Let $E/\mathbb{Q}$ be finite abelian with group G and degree n. Fix an odd prime p. Let O be the integers in a finite extension $J/\mathbb{Q}_p$ containing the values of the characters of G, and put $D = J/O$. For a character α of G write $S_{\alpha,r}$ for the subgroup of $H^1(\mathbb{Q}, D(\alpha^{-1}\kappa_p^{-r}))$ consisting of classes zero on inertia away from p and on the decomposition group at p. Write $M_{p,r}(E)$ for the sign $(-1)^r$ in the strict group over E with coefficients $(\mathbb{Q}_p/\mathbb{Z}_p)(-r)$. All valuations below have $v_p(p) = 1$.

Lemma 25.22 (Integral comparison with all the scalar groups)**.** *There are maps in both directions between $M_{p,r}(E) \otimes O$ and $\bigoplus_{\alpha(c)=(-1)^r} S_{\alpha,r}$, with both composites multiplication by n. On the summand indexed by α, the action of a deck transformation g of $E/\mathbb{Q}$ is $\alpha(g)$. In particular, for any projector formed from averages over subgroups of order prime to p, an exponent p^a on its scalar images gives exponent $p^{a+v_p(n)}$ on its image over E.*

Proof. The induced coefficient over $\mathbb{Q}$ is $U = D[G] \otimes \kappa_p^{-r}$, where $D[G]$ denotes one copy of D for each $g \in G$. Arithmetic translation on the basis is $e_g \mapsto e_{hg}$ for $h \in G$. The commuting deck action of $t \in G$ is $e_g \mapsto e_{gt^{-1}}$. Shapiro's lemma gives the degree-one cohomology over E. Indeed evaluation at the identity coset on restricted cochains is the Shapiro map. Translation of that coset gives the usual action on the classes by conjugation and transport of coefficients. For a decomposition or inertia group I, its orbits on the cosets give a direct sum of induced modules for the stabilizers $I \cap gG_Eg^{-1}$. Evaluation on each orbit identifies the restriction map with the restrictions at all corresponding places of E. Applying this at the decomposition group above p and at every inertia group away from p proves the assertion for the strict local conditions, including at primes ramified in E. Extension from $\mathbb{Z}_p$ to O commutes with these kernels since O is finite free.

Suppress the common twist. On tuples in the indicated copies of D use the two maps

$$(x_g)_g \longmapsto \left(\sum_g \alpha(g)^{-1} x_g\right)_\alpha, \qquad (y_\alpha)_\alpha \longmapsto \left(\sum_\alpha \alpha(g) y_\alpha\right)_g.$$

Their entries belong to O. Arithmetic translation acts on each output of the first map by $\alpha(h)^{-1}$, and deck translation by $\alpha(t)$. The maps commute with the coefficient actions in both directions. Character orthogonality gives both composites n on the coefficient modules, hence on cohomology and on its strict kernels. Project to the prescribed sign using the idempotent for complex conjugation, since 2 is a unit. For the final assertion apply both maps to the projected module. A scalar bound on the first image kills n times that module. The prime-to-p part of n acts invertibly, and faithful flatness descends the resulting bound to $\mathbb{Z}_p$. □

Theorem 25.23 (An integral scalar annihilator with ramified character values)**.** *Let $\chi = \alpha^{-1}$ be primitive of conductor f. Suppose $k \geq 2$, $\alpha(c) = (-1)^k$, and $\bar{\chi}\bar{\kappa}_p^k \neq 1$, where the bar denotes reduction in the residue field of O. There is a positive integer b prime to fp and a series $F \in O[[X]]$ such that, on putting $X_s = (1+p)^s - 1$ and $A(s) = F(X_s)$, one has*

$$A(r+1)S_{\alpha,r} = 0 \quad (r \geq 1,\ p-1 \mid r+k).$$

For every $K = k + j(p-1)$, $j \geq 0$, the same series satisfies

$$A(1-K) = b^{1-K}(b^K - \chi(b)^{-1})(1 - \chi(p)p^{K-1})\,\frac{B_{K,\chi}}{K}.$$

The factors preceding the Bernoulli value are units of O, with $\chi(p) = 0$ if $p \mid f$.

Proof. Choose a unit residue b modulo $\operatorname{lcm}(f,p)$ on which $\bar{\chi}(b)\bar{b}^k \neq 1$, and take a positive representative. Fix an admissible r and put $\theta = \chi\kappa_p^{-r}$. Some Galois element has $\theta(\tau)-1 \in O^\times$, so $D(\theta)^{G_\mathbb{Q}} = 0$. For $l \geq 1$ the coefficient sequence for multiplication by p^l therefore gives a unique finite-coefficient lift of each strict class killed by p^l. Set $m = \operatorname{lcm}(f, p^l)$ and $L = \mathbb{Q}(\zeta_m)$. Restriction of the lift to L is injective. A cocycle z inflated from the abelian quotient $\mathrm{Gal}(L/\mathbb{Q})$ satisfies $(\theta(\tau)-1)z(g) = (\theta(g)-1)z(\tau)$ modulo p^l, and is a coboundary. This proves injectivity by inflation–restriction.

Choose a generator of μ_{p^l}. Kummer theory identifies the restricted lift with an element of $(L^\times/L^{\times p^l}) \otimes_{\mathbb{Z}/p^l} (O/p^lO)$ of character $\beta = \kappa_p\theta^{-1} \bmod p^l$. The factor κ_p acts on the chosen root and θ^{-1} comes from conjugation on the argument of the restricted homomorphism. Away from p the divisible class is a coboundary on inertia. On the inertia of L the whole character θ is trivial, so the finite lift restricts to zero there. A Kummer representative then acquires a p^l-th root over an unramified extension, and its valuation is divisible by p^l. At $w \mid p$ the finite homomorphism on G_{L_w}, viewed inside D, has the form $(\kappa_p^{-r} - 1)y$ because the divisible class is locally zero and L kills χ. It factors through the cyclotomic image. Lemma 24.5 gives a unit representative in each coordinate of O/p^lO, a free $\mathbb{Z}/p^l$-module. Thus division of the principal ideal by its exponent defines the equivariant map $(a) = \mathfrak{a}^{p^l} \mapsto [\mathfrak{a}]$. Its kernel consists of global unit classes. On the odd part those are generated by roots of unity, since $u/\bar{u}$ is a root of unity for each global unit and 2 is invertible. The roots have character κ_p, whereas β differs from it by a unit at τ. As $\beta(c) = -1$, this proves injection on the required classes.

The integral Stickelberger element $(b - \sigma_b)\Theta_m$ kills the class group of L, as in Theorem 24.3. Its action on this eigengroup is the sum over units $1 \leq a \leq m$ of $\lfloor ba/m \rfloor \chi(a) a^{-r-1} \bmod p^l$. This argument uses an eigengroup defined by equations and requires no division by a group order.

Write f_0 for the prime-to-p part of f. On $(\mathbb{Z}/f_0\mathbb{Z})^\times \times \mathbb{Z}_p^\times$ use the bounded measure which assigns $\lfloor ba/m \rfloor - (b-1)/2$ to the unit cylinder $a \bmod m$, for $m = f_0p^v$, $v \geq \max(1, v_p(f))$. Summing the floors over the p lifts adds $(p-1)(b-1)/2$ to the old floor, since multiplication by b permutes residues modulo p. This gives compatibility and the measures have p-integral values. Integrate

$$\chi(a)\omega(a_p)^{k-1}\langle a_p\rangle^{-s}, \qquad \langle a_p\rangle = a_p/\omega(a_p).$$

The integrand is odd, so the constant correction cancels in each relevant finite sum. At $s = r+1$ the integral reduces to the Stickelberger sum modulo p^l. This proves annihilation on all elements of the scalar group. Write $\langle a_p\rangle = (1+p)^u$, $u \in \mathbb{Z}_p$, and expand $(1+X_s)^{-u}$ in integral binomial coefficients. Uniform convergence for $X_s \in p\mathbb{Z}_p$ permits termwise integration and gives $F \in O[[X]]$.

At $s = 1-K$ the integrand at integer representatives is $\chi(a)a^{K-1}$. Put $w_a = ba - m\lfloor ba/m \rfloor$. These representatives permute the units. Expanding w_a^K and dividing by m gives, up to a term tending to zero,

$$Kb^{K-1}\sum_a \chi(a)a^{K-1}\lfloor ba/m \rfloor = (b^K - \chi(b)^{-1})\, m^{-1}\sum_a \chi(a)a^K + o_p(1).$$

Here $o_p(1)$ denotes a quantity tending to zero p-adically as $v \to \infty$, with K fixed. Summing the powers first on the progressions modulo f gives the limit $B_{K,\chi}$ when all residues are allowed, by the Bernoulli polynomial difference and derivative formulas in Theorem 25.9. If $p \nmid f$, deletion of the multiples of p subtracts $\chi(p)p^{K-1}B_{K,\chi}$. If $p \mid f$, such terms already have character value zero. This proves the formula. The Euler factor is a unit since $K \geq 2$, and the choice of b works for all these K because they agree modulo $p-1$. □

Proposition 25.24 (Higher finite differences and the full scalar exponent)**.** *In Theorem 25.23 put $u_j = A(1-k-j(p-1))$ and $y = (r+k)/(p-1)$. Let $\Delta u_j = u_{j+1} - u_j$. For every $h \geq 1$ one has*

$$A(r+1) \equiv \sum_{j=0}^{h-1} \binom{-y}{j} \Delta^j u_0 \pmod{p^h O}.$$

If this residue is nonzero then $p^h S_{\alpha,r} = 0$. In particular suppose $u_0 \in pO$, and denote the residues of u_0/p and $(u_1 - u_0)/p$ in O/pO by a_0, a_1. If $a_0 \notin \mathbf{F}_p a_1$, then $p^2 S_{\alpha,r} = 0$ for every positive $r \equiv -k \bmod (p-1)$. When $O/\mathbb{Z}_p$ is unramified the sharper bound $pS_{\alpha,r} = 0$ holds on this entire class of twists.

Proof. In the measure just constructed, $\Delta^j u_0$ is the integral of $\chi(a)a_p^{k-1}(a_p^{p-1}-1)^j$, hence belongs to $p^j O$. Multiply $\chi(a)a_p^{k-1}$ by the binomial expansion of $(1+(a_p^{p-1}-1))^{-y}$. This recovers the integrand at $r+1$, and its terms from index h onward lie uniformly in $p^h O$. If the residue is nonzero, the valuation of the annihilator is less than h, so it divides p^h in O. For the last assertion the residue of $A(r+1)/p$ is $a_0 - ya_1$. Only elements of the prime field occur as residues of the ordinary integer y. Under the stated condition the annihilator belongs to pO and lies outside $p^2 O$. In an unramified valuation ring this gives valuation exactly one. □

Corollary 25.25 (A quartic character at eleven)**.** *Let χ be the character modulo 41 with $\chi(6) = i$. For $p = 11$ the full scalar groups $S_{\chi^{-1},r}$ are killed by 11 for every positive $r \equiv 2 \bmod 10$.*

Proof. Modulo 41, the powers $6^{20} = -1$, $6^8 = 10$ show that 6 has order forty. Take $k = 8$, $O = \mathbb{Z}_{11}[i]$ and $b = 12$. The ring is unramified of degree two since -1 is a nonsquare modulo eleven. As $12 = 6^{27} \bmod 41$ its character value is $-i$, giving the required smoothing unit. The following four columns are enough to reproduce the two moment reductions. For row e and column j, sum $\lfloor 12t/4961 \rfloor t^e$ modulo 121 over $1 \leq t \leq 4961 = 41 \cdot 121$, $11 \nmid t$, and $t \bmod 41 \in \{6^{4a+j} : 0 \leq a < 10\}$.

$e \backslash j$	0	1	2	3
7	15	29	59	95
17	70	117	114	84

For an alternative direct evaluation the Bernoulli polynomial formula gives $B_{8,\chi}/8 = 1705510378 + 4864413026i$. Combining the columns with the weights $1, i, -1, -i$ gives $u_0 = 77+55i$ and $u_1 = 77+33i$ modulo 121. Thus $a_0 = 7+5i$, $a_1 = 9i$ in $\mathbf{F}_{121}$. Every $a_0 - ya_1$ for $y \in \mathbf{F}_{11}$ has real coordinate seven. Proposition 25.24 proves the assertion. □

25.10 Omitted Euler factors at the nonpositive integers

A long vertical theta string can put the argument of a Hecke function at zero in a horizontal doubling integral. The finite places removed from that integral then matter. We record the calculation for the CM fields and angular characters in the manuscript.

Proposition 25.26 (A split Euler factor and the functional equation)**.** *Let $E/\mathbb{Q}$ be abelian CM of degree $2f$. At a choice of one embedding τ from each conjugate pair, let a unitary Hecke character ρ have infinity factors $(z/|z|)^{2a_\tau}$, with $a_\tau \in \mathbb{Z}$ and some $a_\tau \neq 0$. If w lies over a completely split rational prime p and ρ is unramified at w, put $z_w = \rho_w(\varpi_w)$, $J = E(z_w)$ and $D = [J:\mathbb{Q}]$, using a fixed inclusion $E \subset \mathbb{C}$. Then J is a number field and*

$$|1 - z_w| \;\geq\; 2^{1-D/2} p^{-[J:E]\sum_\tau |a_\tau|/2} > 0.$$

In fact z_w has infinite order. Let S_E be a finite set of primes over completely split rational primes, and put $A = |D_E| N\mathfrak{f}_\rho$. For $u \geq 0$ integral with $M_\tau = |a_\tau| > u$ for every τ, one has

$$|L_E^{S_E}(-u,\rho)| = A^{u+1/2}(2\pi)^{-f(2u+1)} \prod_\tau \prod_{b=-u}^{u} (M_\tau + b)\, |L_E^{S_E}(1+u,\bar\rho)|$$
$$\times \prod_{\substack{w \in S_E \\ \rho_w \text{ unramified}}} \frac{|1 - z_w (Nw)^u|}{|1 - \bar z_w (Nw)^{-1-u}|} > 0.$$

The first bound applies at each omitted place when $u = 0$.

Proof. Let H be the order of the class of w in the ray class group modulo the conductor of ρ. We can write $w^H = (\alpha)$ with $\alpha \equiv 1 \bmod \mathfrak{f}_\rho$. Evaluate the character on the principal idele α. At the conductor primes its residue is trivial and at the other primes only w contributes. Thus

$$z_w^H = \prod_\tau \left(\frac{\tau(\alpha)}{\bar\tau(\alpha)} \right)^{-a_\tau}.$$

All embeddings on the right may be viewed as automorphisms of E. The ideals $\tau w, \bar\tau w$ as τ varies are pairwise distinct since the decomposition group of w is trivial. The valuations of the right side at these two primes are $-Ha_\tau, Ha_\tau$. This proves algebraicity and gives a nonzero valuation at some prime, excluding every root of unity. At each embedding of E the numerator and denominator in each ratio are complex conjugates, since conjugation is central in $\mathrm{Gal}(E/\mathbb{Q})$. All conjugates of z_w in $\mathbb{C}$ therefore have absolute value one.

At a prime of J over τw the valuation of z_w is $-a_\tau$ times its ramification index. Over $\bar\tau w$ the sign is reversed. There are no other nonzero valuations. Using the local degree formula, the denominator ideal of z_w in J has absolute norm $p^{[J:E]\sum_\tau |a_\tau|}$. The denominator of $1 - z_w$ divides this ideal. Its numerator ideal has norm at least one. In the field norm of $1 - z_w$ the chosen embedding of J and its complex conjugate contribute $|1 - z_w|^2$. Each of the other $D - 2$ absolute factors is at most two. Comparing the two estimates for the absolute norm gives the asserted bound.

The completed Hecke function has conductor factor $A^{z/2}$ and gamma factors $\Gamma_{\mathbb{C}}(z + M_\tau)$, where $\Gamma_{\mathbb{C}}(z) = 2(2\pi)^{-z}\Gamma(z)$. Take absolute values in the functional equation at $z = -u$. The root number has modulus one. Each quotient of gamma factors contributes $(2\pi)^{-(2u+1)} \prod_{b=-u}^{u} (M_\tau + b)$ by the gamma recurrence, since $M_\tau - u > 0$. Restoring the omitted Euler factors at $1 + u$ and removing the ones at $-u$ gives the second formula. The value on the positive side is nonzero by absolute convergence for $u > 0$, and by Lemma 72.9 for $u = 0$. For $u > 0$ the numerator of each correction factor is at least $(Nw)^u - 1$; the denominators are positive for every $u \geq 0$. The preceding split-prime argument handles the remaining numerator at $u = 0$. Tate, global functional equation for Hecke characters. □

26 Norms and cyclic character fields

26.1 Norms of ideal classes and the exponents of strict classes

Fix one of the fields E of Section 24.7 and an odd prime p. Write $G = \mathrm{Gal}(E/\mathbb{Q}) = P \times H$, where P is the p-Sylow subgroup, and put $K = E^H$, $a = \log_p |P|$. Choose an unramified coefficient ring O with fraction field J and residue field $\mathbf{f}$ containing the required roots of unity of order prime to p (in O we use their Teichmüller lifts). For $\alpha \in \widehat{H}$, extend α trivially over P. At a complementary twist $r \geq 1$ we have $\alpha(c) = (-1)^r$. On G_K write

$$\theta = \alpha^{-1}\kappa_p^{-r} = \tau\langle\kappa_p\rangle^{-r}, \qquad \tau = \alpha^{-1}\omega^{-r}, \qquad \kappa_p = \omega\langle\kappa_p\rangle.$$

Here ω is the Teichmüller character and $\langle\kappa_p\rangle$ takes values in $1+p\mathbb{Z}_p$. Let S_α be the strict group with coefficients $(J/O)(\theta)$ over K. By Lemma 24.8 it is the α-summand of the original strict group on E after extension to O. This descent includes primes dividing $[E:\mathbb{Q}]$.

Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension, with layer $\mathbb{Q}_i$ of degree p^i. Set

$$L = (E(\mu_p))^+, \qquad [K \cap \mathbb{Q}_\infty : \mathbb{Q}] = p^d, \qquad L_i = L\mathbb{Q}_{d+i}, \qquad L_\infty = L\mathbb{Q}_\infty.$$

The field K is totally real, L/K has degree prime to p, and the even character τ factors through $\Delta = \mathrm{Gal}(L/K)$. We may equally use the smaller field cut out by $\ker\tau$ over K in place of L. In either case $L \cap \mathbb{Q}_\infty = K \cap \mathbb{Q}_\infty$, by the prime-to-$p$ degree. Thus $\mathrm{Gal}(L_\infty/K) = \Delta \times \Gamma$, where $\Gamma = \mathrm{Gal}(L_\infty/L)$. Choose the generator γ mapping to $(1+p)^{p^d}$ under the principal cyclotomic character. Put

$$u = (1+p)^{-rp^d}, \qquad h = v_p(u-1) = 1 + d + v_p(r), \qquad n_0 = a - d.$$

The valuation follows by taking the p-adic logarithm for odd p. Every place over p is totally ramified in L_m/L_n for $m \geq n \geq n_0$. Indeed inertia at p surjects onto $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Passing to a completion L_w replaces the absolute inertia subgroup by one of index $e(L_w/\mathbb{Q}_p)$. The index of its image in the cyclotomic group therefore divides this ramification index and has p-part at most p^a. It follows that its image contains $\Gamma^{p^{a-d}}$.

Write $A_i = \mathrm{Cl}(\mathcal{O}_{L_i}[1/p])\{p\}$. These are the ordinary p-primary ideal class groups modulo the classes of the primes above p. Define

$$C_i = e_\tau(A_i \otimes_{\mathbb{Z}_p} O), \qquad e_\tau = |\Delta|^{-1} \sum_{z \in \Delta} \tau(z)^{-1} z.$$

We use the unramified ring O large enough for the characters under consideration. At fixed E, p, the fields L_i in the larger choice above work for every α, r.

Lemma 26.1 (Strict classes over the cyclotomic tower)**.** *With transition maps induced by ideal norms, there is an identification*

$$S_\alpha = \varinjlim_{i \geq n_0} \mathrm{Hom}_O(C_i/(\gamma - u)C_i, J/O). \tag{26.1}$$

The maps on the right are injective. The formula also holds when τ is trivial on a decomposition group above p.

Proof. Over L_∞ the action on $D = (J/O)(\theta)$ is trivial. Restriction identifies $H^1(K, D)$ with the equivariant continuous homomorphisms from G_{L_∞} to D. For this assertion use inflation–restriction. The quotient $\Delta \times \Gamma$ has vanishing H^2 on D, because averaging removes the prime-to-p factor and $\mathbb{Z}_p$ has p-cohomological dimension one. Its H^1 also vanishes. Indeed D^Δ is

zero or all of D, and multiplication by $u-1\neq 0$ is surjective on the divisible module D. This computes the procyclic H^1. At a place over p the same argument gives injectivity on restriction in H^1. Its decomposition quotient is a product of a prime-to-p group and an open subgroup of Γ. The corresponding power of u still differs from one. On inertia away from p the quotient in L_∞/K has order prime to p, so restriction there is injective as well.

Represent a strict class by a continuous cocycle f. Its image is finite by compactness. At each of the finitely many places of K over p it is a coboundary $(\theta(g)-1)b_w$. Choose i large enough that $\theta(G_{L_i})$ acts trivially on the image of f and on all b_w. Then f restricts to a homomorphism on G_{L_i}, zero on the decomposition groups over p. For conjugate places the cobounding elements differ from translates of the chosen elements by values of f, so the same i works. Away from p the cocycle is a coboundary on inertia and θ is trivial on inertia over L_i. The restricted homomorphism is consequently unramified there. Global reciprocity at the finite layer now factors it through A_i. [4]

Let H_i' be the class field of A_i. It is the maximal abelian unramified p-extension of L_i split at all places over p. The archimedean distinction has order a power of two. For $i\geq n_0$, total ramification gives $H_i'\cap L_\infty=L_i$. Thus G_{L_∞} surjects onto A_i. Conjugation of the restricted cocycle on this group selects the character τ of Δ and imposes $f(\gamma z)=uf(z)$. These are exactly the relations on the right side of (26.1). Conversely, a homomorphism there gives an equivariant homomorphism on G_{L_∞} and hence a unique global class. It satisfies the two local conditions by the local injectivity just proved. Base change sends $H_i'L_m$ into H_m' for $m\geq i$, and restriction of class field automorphisms is the ideal norm. Surjectivity on A_i follows from $H_i'\cap L_m=L_i$. This proves the formula and the injectivity of its maps. □

Lemma 26.2 (Relations at two successive layers)**.** *For $m\geq n\geq n_0$ let $Y_{m,n}=\ker(A_m\to A_n)$. Write $g=\gamma^{p^n}$ acting on A_m, and $\nu_n=1+g+\cdots+g^{p-1}$. For $m\geq n+1$,*

$$(g-1)A_m\ \subseteq\ Y_{m,n},\qquad Y_{m,n+1}=\nu_nY_{m,n}. \tag{26.2}$$

Proof. The field H_m' is Galois over L_n by the defining maximal property of the class field. A decomposition group of a prime over p maps isomorphically onto $\mathrm{Gal}(L_m/L_n)$, since the prime splits in H_m'/L_m and is totally ramified in L_m/L_n. Choose one such group and lift g to its generator s. The full group is the semidirect product of A_m by $\langle s\rangle$. For each prime $w\mid p$ of L_n, choose one prime above it in H_m'. The generator of its decomposition group mapping to g has the form z_ws with $z_w\in A_m$, written additively. For the reference prime $z_w=0$.

Abelianizing imposes $(g-1)A_m=0$. Killing the decomposition groups then imposes $s=1$ and $z_w=0$ for every w. The resulting extension of L_n is unramified outside p and split at p. It is exactly H_n', since $H_n'L_m$ is contained in H_m'. Hence

$$Y_{m,n}=(g-1)A_m+\sum_{w\mid p}\mathbb{Z}_pz_w.$$

There is a unique prime of L_{n+1} above each w. Its decomposition generator for the next base is $(z_ws)^p=(\nu_nz_w)s^p$. The same presentation, now with $g^p-1=\nu_n(g-1)$, gives (26.2). □

Let $J_n=\ker(C_{n+1}\to C_n)$. The following integer counts generators of the relative class group after reducing both the coefficients and the cyclotomic action. It is given by

$$\rho_n(\tau)=\dim_{\mathbf{f}}J_n/(pJ_n+(\gamma-1)J_n)\qquad(n\geq n_0).$$

Theorem 26.3 (Bounds for high elementary divisors)**.** *The sequence $\rho_n(\tau)$ is nonincreasing. At every $n\geq n_0$ the number of elementary divisors of S_α strictly larger than p^{h+n}, measured*

over O, is at most $\rho_n(\tau)$. If $C_{n+1} \to C_n$ is an isomorphism, then all $C_m \to C_n$ for $m \ge n$ are isomorphisms and

$$S_\alpha \simeq \mathrm{Hom}_O\left(C_n/(\gamma-u)C_n, J/O\right), \qquad p^{h+n}S_\alpha = 0. \tag{26.3}$$

This one equality of class-group orders applies to every twist with the same τ.

Proof. Put $Y^\tau_{m,n} = e_\tau(Y_{m,n} \otimes O)$, and write $\mathfrak{m} = (p, \gamma - 1)$ for the indicated operators. Surjectivity of norms and Lemma 26.2 identify $J_n = Y^\tau_{m,n}/\nu_n Y^\tau_{m,n}$ whenever $m \ge n+1$. Since $\nu_n \equiv p \bmod (\gamma - 1)$, it follows that

$$Y^\tau_{m,n}/\mathfrak{m}Y^\tau_{m,n} \simeq J_n/\mathfrak{m}J_n.$$

For $m \ge n+2$, multiplication by ν_n surjects from $Y^\tau_{m,n}$ onto $Y^\tau_{m,n+1}$. Reduction modulo $\mathfrak{m}$ proves monotonicity. If the displayed dimension is zero, $\gamma - 1$ acts surjectively on $Y^\tau_{m,n}/p$. It also acts nilpotently there since γ has p-power order. Thus $Y^\tau_{m,n}/p = 0$, which forces the finite group to vanish. In particular $J_n = 0$ gives the stabilization in the statement.

Put $B_m = C_m/(\gamma - u)C_m$. In this module $\gamma^{p^n} - 1$ acts by $u^{p^n} - 1$, of valuation $h + n$. By (26.2), $p^{h+n}B_m$ is contained in the image I of $Y^\tau_{m,n}$ in B_m. On I/pI both p and $\gamma - 1$ vanish. Hence $\dim_{\mathbf{f}} I/pI \le \rho_n(\tau)$. The subgroup $(p^{h+n}B_m)[p]$ injects into $I[p]$, which has the same dimension as I/pI by the elementary divisor theorem over O. This bounds the number of long summands of B_m, and likewise of its O-dual into J/O. The strict group is finite by the number-ring comparison of Section 25.1 and finiteness of the even K-group there. Lemma 26.1 therefore attains the whole group at some finite m, which may be increased beyond n. This proves the bound. Under stabilization all the norms are equivariant isomorphisms, so the limit is the dual at n. Here $\gamma^{p^n} = 1$ on C_n, proving the stated exponent. □

26.1.1 An exact nonzero component in every matching twist

Write χ_D for the primitive quadratic character of fundamental discriminant D.

Proposition 26.4. *For $k = \mathbb{Q}(\sqrt{67})$, $k_i = k\mathbb{Q}_i$ in the cyclotomic $\mathbb{Z}_3$-extension, one has*

$$|\,\mathrm{Cl}(\mathcal{O}_{k_i}[1/3])\{3\}| = 3 \qquad (i \ge 3).$$

The nonidentity element of $\mathrm{Gal}(k/\mathbb{Q})$ acts by inversion on these groups.

Proof. We use Theorem 2 of Fukuda and Komatsu for a real quadratic field in which p splits. Let $\mathfrak{p}^{h_k} = (z)$, where h_k is its ordinary class number, and let ε be a fundamental unit. In the completion at the conjugate prime write $n_1 = v_p(z^{p-1} - 1)$, $n_2 = v_p(\varepsilon^{p-1} - 1)$. In the range $2 \le n_1 < n_2$ the theorem applies if $p \nmid h_k$ and the p-class group of $k(\mu_p)$ is elementary abelian. For $i \ge n_1 + n_2 - 2$ it gives $(A : D) = p^{n_1 - 1}$, where $A = \mathrm{Cl}(k_i)\{p\}$ and D is its subgroup represented by powers of the prime above $\mathfrak{p}$. [11, Thm. 2, pp. 95–96]

Here $p = 3$ splits, since $67 \equiv 1 \bmod 3$. The ring of integers is $\mathbb{Z}[\sqrt{67}]$, of discriminant 268. Minkowski's bound $\sqrt{268}/2 < 9$ shows that prime ideals of norm at most eight generate its class group. The prime 5 is inert. The elements $221 + 27\sqrt{67}$, $8 + \sqrt{67}$ and $90 + 11\sqrt{67}$ have norms $-2, -3, -7$. Together with their conjugates they generate the prime ideals needed over $2, 3, 7$, so $h_k = 1$. Take $z = 8 + \sqrt{67}$. The continued fraction

$$\sqrt{67} = [8; \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}]$$

gives $\varepsilon = 48842 + 5967\sqrt{67}$ from the first full period by the continued-fraction theorem for Pell's equation. Norm -1 is impossible by reduction modulo four. In the completion where z is

a unit we have $\sqrt{67} \equiv 38 \bmod 81$, since this is a root with residue -1 mod 3 and the derivative is a unit. Therefore $z \equiv 46$, $\varepsilon \equiv 26 \bmod 81$. Squaring and subtracting one gives $n_1 = 2$ and $n_2 = 3$.

The biquadratic field $k(\mu_3)$ has the other quadratic subfields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-201})$. The former has class number one. The latter has discriminant -804 and class number twelve. For a direct check the leading coefficients of its reduced positive primitive forms, with multiplicities, are

$$1,\ 2,\ 3,\ 5,\ 5,\ 6,\ 7,\ 7,\ 10,\ 10,\ 14,\ 14.$$

Indeed in a form (A, B, C) take $A \le \sqrt{804/3} < 17$, $|B| \le A$, $C = (B^2 + 804)/(4A)$ integral and at least A, and $\gcd(A, B, C) = 1$. At $|B| = A$ or $A = C$ take $B \ge 0$. These give respectively $B = 0, 2, 0, \pm 4, 6, \pm 6, \pm 6, \pm 6$ for the eight distinct leading coefficients above. The classification of reduced binary quadratic forms gives the count. On the 3-class group of the biquadratic field the four character idempotents are integral at 3. The invariant subgroup for each quadratic involution descends to its fixed field because extension and norm compose in the two directions to multiplication by two and to the sum of the involution and the identity. The common rational summand is trivial. Hence the whole 3-part is the one from $\mathbb{Q}(\sqrt{-201})$, of order three and elementary abelian. All hypotheses of the quoted theorem now hold.

The unique prime over 3 of $\mathbb{Q}_i$ is principal. A generator is the relative norm of $1 - \zeta_{3^{i+1}}$ from the full cyclotomic field to $\mathbb{Q}_i$, since the residue degree is one. Its extension to k_i is the product of the two primes above 3, each to the first power because 3 splits in k. Their classes are therefore inverse, and A/D is precisely the 3-class group with both primes divided out. The published index formula gives $3^{2-1} = 3$ for $i \ge 3$.

Finally the corresponding group over $\mathbb{Q}_i$ is zero. Apply the presentation in Lemma 26.2 to $\mathbb{Q}_i/\mathbb{Q}$. There is just one prime over 3, so every z_w in that presentation is zero. The bottom group is trivial and the upper group equals its image under $\gamma - 1$, which forces it to vanish by reduction modulo 3 and nilpotence. The quadratic norm and extension argument applies also after inverting 3. It kills the invariant part on k_i. An involution on a group of order three with this property acts by inversion. □

Theorem 26.5 (An exact component on the period fields)**.** *Take $p = 3$. If the primitive character specifying the period field is $\psi = \chi_{268}$, let r run over the positive even integers. If $\psi = \chi_{-804}$, let r run over the positive odd integers. For every field $E = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0})$ in either construction, the ψ-component of the complementary strict group is cyclic of order three at every indicated twist. Its total contribution for $1 \le r < t$ is $\lfloor (t-1)/2 \rfloor \log 3$ in the first case and $\lfloor t/2 \rfloor \log 3$ in the second.*

Proof. The Galois group of $E/\mathbb{Q}$ has order a power of two, so here $K = \mathbb{Q}$ and descent is an isomorphism on every character component over $\mathbb{Z}_3$. The Teichmüller character at 3 is χ_{-3}, and $\chi_{-804} = \chi_{268}\chi_{-3}$. In both cases $\tau = \psi^{-1}\omega^{-r} = \chi_{268}$. Use its field k in Lemma 26.1. Proposition 26.4 says that for $i \ge 3$ the entire group belongs to this character and has order three. Every norm on this part is surjective, hence an isomorphism. The pro-3 group Γ acts trivially on a cyclic group of order three, whose automorphism group has order two. Also $u = 4^{-r} \equiv 1 \bmod 3$. Consequently its quotient by $\gamma - u$ and its dual into $\mathbb{Q}_3/\mathbb{Z}_3$ both have order three. This computes the full group in (26.1). Counting the even or odd integers in the required range gives the two totals. □

26.2 A single relative class group for all twists at a prime

Retain K, L_i, γ, d, n_0 and the coefficient ring O from Section 26.1, using $L = (E(\mu_p))^+$. Fix a character τ of $\Delta = \mathrm{Gal}(L/K)$. Consider finitely many complementary pairs (α_i, r_i) with

residual character τ, taking each pair once. Their positive twists r_i are distinct. Indeed at fixed r the restriction of α to G_K determines α, since G_K surjects onto $\mathrm{Gal}(E/K) = H$. Put

$$u_i = (1+p)^{-r_i p^d}, \qquad h_i = 1 + d + v_p(r_i), \qquad D_i = \sum_{\ell \neq i} (1 + d + v_p(r_i - r_\ell)).$$

An empty sum is zero. The numbers D_i measure the denominators for interpolation at the different u_i.

Theorem 26.6 (One norm bound for several specializations)**.** *Let $n \geq n_0$, $j \geq 1$, and let c_i be integers with $c_i \geq n + h_i + D_i$. Write S_i for the full strict group of the indicated pair, and $C_n = e_\tau(A_n \otimes O)$. Then*

$$\sum_i \log |(p^{c_i} S_i)[p^j]| \;\leq\; \log |\ker(C_{n+j} \longrightarrow C_n)|. \tag{26.4}$$

If the right side is less than $j \log |\mathbf{f}|$, then the same bound holds for $\sum_i \log |p^{c_i} S_i|$.

Proof. Take $m \geq n + j$ large enough for the direct limit in Lemma 26.1 to attain each of the finitely many finite groups S_i. Thus S_i is the O-dual into J/O of $B_i = C_m/(\gamma - u_i)C_m$. Write Y for $\ker(C_m \to C_n)$, and I for its image under the simultaneous quotient map into $\bigoplus_i B_i$. For a given i and $b_i \in B_i$, choose $z_i \in C_m$ mapping to b_i. Apply to it the operator

$$(\gamma^{p^n} - 1) \prod_{\ell \neq i} (\gamma - u_\ell).$$

The result belongs to Y because γ^{p^n} acts trivially on C_n. Its image in every B_ℓ for $\ell \neq i$ is zero. In B_i its image is $(u_i^{p^n} - 1) \prod_{\ell \neq i} (u_i - u_\ell) b_i$. The first factor has valuation $n + h_i$. The difference $u_i - u_\ell$ has valuation $1 + d + v_p(r_i - r_\ell)$ by the principal-unit logarithm. The scalar is therefore $p^{n + h_i + D_i}$ times a unit of O. Varying b_i independently gives

$$\bigoplus_i p^{c_i} B_i \;\subseteq I.$$

Set $g = \gamma^{p^n}$ and $v = 1 + g + \cdots + g^{p^j - 1}$. On B_i this operator acts by $(u_i^{p^{n+j}} - 1)/(u_i^{p^n} - 1)$, of valuation j. It follows that $\bigoplus_i (p^{c_i} B_i)[p^j]$ is contained in the kernel of v on I. For an endomorphism of a finite group the kernel and cokernel have equal orders. Also Y/vY maps onto I/vI. Iterating Lemma 26.2 gives $vY = \ker(C_m \to C_{n+j})$, since the j successive geometric sums multiply to v. Surjectivity of the norms identifies Y/vY with the kernel in (26.4). Dual finite O-modules have the same elementary divisors, which proves the inequality for the S_i. If a group $p^{c_i} S_i$ had exponent at least p^j, its subgroup killed by p^j would contain $O/p^j O$. The strict inequality in the final assertion rules this out for every i, so the displayed truncated orders already give the full orders. □

Corollary 26.7 (Summing over the characters of the period field)**.** *On the common fields and intervals of Volume I, put $\bar{k}_{p,r} = \max(1, k_{p,r})$, where $k_{p,r}$ is the depth in its equation (19.15). For every sufficiently large x, every odd prime p, and every integer $j \geq 1$, one has*

$$\sum_{1 \leq r < t} \log |(p^{\bar{k}_{p,r}} M_{p,r})[p^j]| \;\leq\; \log \frac{|A_{n_0+j}|}{|A_{n_0}|} \;\ll_\psi\; [E : \mathbb{Q}] p^{j+1} \log(2N p^{a+j+1}). \tag{26.5}$$

Here $M_{p,r}$ is the complementary strict group on E, N is its prescribed cyclotomic modulus, and $a = v_p([E : \mathbb{Q}])$.

Proof. For $1 \le r_i < t$, distinct differences on either side of r_i are distinct positive integers after taking absolute values. Consequently

$$D_i \le (t-2)(1+d) + v_p((r_i-1)!(t-1-r_i)!) \le (t-2)(1+d+1/(p-1)).$$

For $p \le P = \exp(x^{\varepsilon}/12)$, the common lower bound for $k_{p,r}$ in Theorem 19.19 is $\lfloor x^{-420} \exp(x^{\varepsilon}/3) \rfloor$. It exceeds $n_0 + h_i + D_i$ uniformly for large x, since $t \le x^{401}$ and $p^a \le \operatorname{ord}(\psi)$. For $p > P$ we have $p > t+1$, $p \nmid N[E:\mathbb{Q}]$ and $K = \mathbb{Q}$. Inertia at p distinguishes the residues $-r$ modulo $p-1$, and hence distinguishes all the twists in this range. Each character τ occurs at most once, giving $D_i = 0$, $h_i = 1$ and $n_0 = 0$.

Apply Theorem 26.6 with $n = n_0$ separately for each τ, then sum. Each summand of $M_{p,r} \otimes O$ occurs once. On the right the integral character idempotents partition the relative class group after extension to O. Divide the logarithms by $[J:\mathbb{Q}_p]$ to undo this extension on both sides. Norm surjectivity gives the first inequality.

For the size estimate put $T = L_{n_0+j}$. It lies in the cyclotomic field of modulus Np^{a+j+1} and has degree at most $[E:\mathbb{Q}](p-1)p^{a-d+j}$. The factor p^{a-d} is bounded by $\operatorname{ord}(\psi)$. The conductor–discriminant formula bounds $\log|\operatorname{disc} T|$ by $[T:\mathbb{Q}]\log(Np^{a+j+1})$. Minkowski's theorem gives an integral representative of each class of norm at most $2^{[T:\mathbb{Q}]}|\operatorname{disc} T|^{1/2}$. The number of ideals of norm at most $B \ge 1$ is at most $B^2\zeta_T(2) \le B^2\zeta(2)^{[T:\mathbb{Q}]}$. These estimates give the asserted upper bound even for the ordinary class number of T. □

At a prime where $k_{p,r} = 0$, the first layer of $M_{p,r}$ enters the original sum separately. Its logarithmic order is exactly $\log|M_{p,r}| - \log|pM_{p,r}|$. The estimate above controls all the twists jointly beyond the stated depths. The elementary class-number bound grows with j, leaving a uniform bound for the full surviving orders to be established.

26.3 Real cyclic quartic and sextic fields

Let $F/\mathbb{Q}$ be totally real and cyclic of degree $m = 4$ or 6, with conductor f. Write k_j for its subfield of degree j, where $j = 2$ in both cases and $j = 3$ also occurs when $m = 6$. Write f_j for the corresponding conductor. Let h_L denote the ordinary ideal class number of a field L and R_L its regulator, with one row deleted in the logarithmic unit matrix. Use the following two quotients.

$$(H, R_*) = \begin{cases} (h_F/h_{k_2},\ R_F/R_{k_2}) & m = 4, \\ (h_F/(h_{k_2}h_{k_3}),\ R_F/(R_{k_2}R_{k_3})) & m = 6. \end{cases}$$

We will bound H, then use the bound to exclude entire primary components from the strict groups in Section 24.7.

Lemma 26.8 (The two faithful characters)**.** *The number H is the order of the joint kernel of the ideal class norms to the maximal proper subfields of F. For a faithful primitive Dirichlet character χ of F,*

$$HR_* = \frac{f}{4}|L(1,\chi)|^2, \qquad H \le \frac{f(\log f)^2}{16R_*}.$$

If $p \nmid m$ and a faithful constituent occurs in $\operatorname{Cl}(F)/p\operatorname{Cl}(F)$, then $p^{\operatorname{ord}_m(p)} \le H$.

Proof. There are two faithful characters, χ and its complex conjugate. Both have conductor f, since both cut out F. The remaining characters come from the indicated proper subfields. The conductor–discriminant formula gives $D_F = f^2 f_2$ for $m = 4$ and $D_F = f^2 f_2 f_3^2$ for $m = 6$, with $D_{k_2} = f_2$ and $D_{k_3} = f_3^2$. Divide the factorization of ζ_F by ζ_{k_2} in the quartic case. In the sextic case take $\zeta_F\zeta_{\mathbb{Q}}/(\zeta_{k_2}\zeta_{k_3})$. The result in either case is $L(s,\chi)L(s,\bar\chi)$. At $s = 1$, the

residue of the zeta function of a totally real field of degree n is $2^{n-1}hR/\sqrt{D}$. The displayed identity follows. Ramaré's inequality $|L(1,\chi)| \le (\log f)/2$ applies since χ is even, primitive and nonprincipal. [5, Cor. 1]

Each extension F/k_j has prime degree and ramifies at a finite place. Indeed $D_F/D_{k_j}^{[F:k_j]} > 1$ by the discriminants above, since $f_j \mid f$ and each proper subfield listed here has conductor greater than one. Thus F meets the ordinary Hilbert class field of k_j in k_j. Its compositum with F is unramified abelian over F and split at real places. Restriction onto its Galois group from the Hilbert class field of F is surjective. By functoriality of the Artin map this is surjectivity of the class norm to k_j. [4]

For $m = 6$ the joint norm is also onto. An extended ideal class from k_2 has norms $(u^3, 1)$, and one from k_3 has norms $(1, v^2)$. The cross norm is principal because the conjugates from one subfield run through its full Galois group over $\mathbb{Q}$, giving the extension of its rational ideal norm. This identity can be checked on ideals after extension to F, where extension of fractional ideals is injective. On each primary part either cubing or squaring is invertible. The image therefore contains one direct factor, and its projection onto the other is onto. This proves the assertion about H.

Finally the action on each norm target factors through a proper quotient of $\mathrm{Gal}(F/\mathbb{Q})$. On the p-parts, the projector to the faithful characters is defined integrally over $\mathbb{Z}_p$ by summing their character idempotents in a splitting ring. The sum is invariant under Galois conjugation and m is a unit. Its image on $\mathrm{Cl}(F)\{p\}$ belongs to the joint kernel and reduces onto the faithful part modulo p. Each faithful irreducible over $\mathbf{F}_p$ has dimension $\mathrm{ord}_m(p)$, the length of the Frobenius orbit of a primitive m-th root of unity. This proves the lower bound. □

Lemma 26.9 (Relative units and discriminants)**.** *There is a unit z generating F as a field with the following properties. Let σ generate $\mathrm{Gal}(F/\mathbb{Q})$, and set $s = \log|z|$ and $t = \log|\sigma z|$ at one fixed real embedding. Then $R_* \ge Q$, where*

$$Q = \begin{cases} s^2 + t^2 & m = 4, \\ s^2 - st + t^2 & m = 6. \end{cases}$$

In the quartic case,

$$\log(f\sqrt{f_2}) \le \log 16 + \sqrt{10}\sqrt{Q}. \tag{26.6}$$

In the sextic case,

$$\begin{aligned} \log(f\sqrt{f_2 f_3}) &\le \log 216 + \sqrt{208/3}\sqrt{Q}, \\ \log(f f_3/f_2) &\le \log 4 + 4\sqrt{Q}, \\ \log(f\sqrt{f_2}/f_3) &\le \log 8 + (4/\sqrt{3})\sqrt{Q}. \end{aligned} \tag{26.7}$$

Proof. Put $U_L = \mathcal{O}_L^\times/\{\pm 1\}$ and let W be the joint kernel of the norms from U_F to the indicated U_{k_j}. Dirichlet's unit theorem realizes U_F as a full lattice in the real hyperplane of coordinate sum zero. The embedded subfield lattices map by the norms onto subgroups of finite index in the product of the subfield lattices. On their own factor these maps are multiplication by $[F : k_j]$ and the cross norms are zero. Thus W has rank two. Its logarithmic vectors, in cyclic order, have the form

$$(s, t, -s, -t) \quad \text{or} \quad (s, t, t - s, -s, -t, s - t),$$

respectively. For degree six the norm to k_3 makes opposite coordinates negatives of each other, while the norm to k_2 makes the sum of the even coordinates zero. Thus σ on W satisfies $\Phi_m(\sigma) = 0$. The irreducible polynomial Φ_m has degree two, so $W \otimes \mathbb{Q}$ has dimension one over

$\mathbb{Q}(\zeta_m)$. Hence W is a fractional ideal up to scaling in $\mathbb{Z}[\zeta_m]$. This ring is Euclidean in both cases (the Gaussian or Eisenstein integers). Choose a generator and represent it by $z \in \mathcal{O}_F^\times$. Then $z, \sigma z$ give a basis of W. If z belonged to a maximal proper subfield, its norm there would make a positive power of z equal to ± 1, contradicting its nonzero logarithm. Hence $\mathbb{Q}(z) = F$.

The logarithmic covolume of U_L is $\sqrt{[L:\mathbb{Q}]}R_L$ for a totally real field. Indeed all its signed maximal minors agree up to sign and the square of the covolume is their sum of squares. The subfield spaces and the relative space are mutually orthogonal by summing logarithms over the norm fibers. In degree four the embedded quadratic lattice has length $2R_{k_2}$. The two basis vectors of W are orthogonal of squared length $2Q$. The index of the sum of the subfield and relative lattices is at most two, by the norm modulo $2U_{k_2}$. Its kernel modulo the subfield lattice is exactly W, since subtracting a subfield unit with that norm leaves norm zero. It follows that $R_* \geq (2R_{k_2})(2Q)/(2\sqrt{4}R_{k_2}) = Q$.

In degree six the embedded subfield covolumes are $\sqrt{6}R_{k_2}$ and $2\sqrt{3}R_{k_3}$, since their logarithmic coordinates are repeated three and two times respectively. The two relative basis vectors have squared length $4Q$ and inner product $2Q$, so their area is $2\sqrt{3}Q$. The quotient by all three lattices injects by the norms into $U_{k_2}/3U_{k_2} \times U_{k_3}/2U_{k_3}$. Indeed if the two norms are divisible by three and two, subtracting the corresponding subfield units leaves an element of W. The index is at most $3 \cdot 2^2 = 12$. Multiplying the three covolumes and dividing by $12\sqrt{6}R_{k_2}R_{k_3}$ yields $R_* \geq Q$.

For the discriminants we record a determinant estimate. List the conjugates x_i of z with logarithms of their absolute values $\lambda_1 \leq \cdots \leq \lambda_n$. Put $S = \sum_i (i-1)\lambda_i$. Then

$$\prod_{i<j} |x_i - x_j| \leq n^{n/2} e^S.$$

To see this, put $b_1 = 0$, $b_{j+1} - b_j = \lambda_j$ and $a_i = (i-1)\lambda_i - b_i$. The exponent $(j-1)\lambda_i - b_j$ is maximized at $j = i$, as its successive differences are $\lambda_i - \lambda_j$. Multiplying the rows and columns of the Vandermonde matrix by e^{-a_i} and e^{-b_j} gives rows of norm at most $\sqrt{n}$. Hadamard's inequality gives the claim since $\sum_i (a_i + b_i) = S$. The square of the Vandermonde product is the discriminant of $\mathbb{Z}[z]$, a multiple of D_F by the index formula. In degree four, if $A \geq B$ are $|s|, |t|$ in decreasing order, $S = 3A + B \leq \sqrt{10Q}$. This gives (26.6).

In degree six the three nonnegative logarithm magnitudes, one for each opposite pair, have the form $A + B, A, B$ with $A \geq B \geq 0$, since they are $|s|, |t|, |s - t|$. Here $Q = A^2 + AB + B^2$. Sorting all six gives $S = 8A + 6B$, and $(208/3)Q - S^2 = (4/3)(2A - 5B)^2 \geq 0$. This proves the first line of (26.7).

For an order $\mathcal{O}_{k_j}[z]$, the relative discriminant is a multiple of $\mathfrak{d}_{F/k_j}$, by the index formula locally at every prime. Thus the product of absolute Vandermonde determinants over the embeddings of k_j is at least $(D_F / D_{k_j}^{[F:k_j]})^{1/2}$. Over each embedding of k_2 the three conjugates have absolute product one. Their logarithms have squared length $2Q$, hence their range is at most $2\sqrt{Q}$ by Cauchy–Schwarz. The three-variable inequality in the proof of Lemma 24.22 bounds each Vandermonde by twice the exponential of that range. Over k_3 each pair has opposite logarithms $\lambda, -\lambda$, so its difference is at most $2e^{|\lambda|}$. The sum of the three magnitudes is $2(A + B) \leq 4\sqrt{Q/3}$, since $4Q - 3(A + B)^2 = (A - B)^2$. These two relative estimates give the remaining lines of (26.7). □

Proposition 26.10 (An upper bound for the joint norm kernel)**.** *For arbitrary conductor, $H < f$ if $m = 4$ and $\log f \geq 16$, or if $m = 6$ and $\log f \geq 90$. For prime conductor $f = p$, $H < p$ if $m = 4$ and $p \geq 64$, or if $m = 6$ and $p \geq 1024$.*

Proof. It suffices to show $\sqrt{Q} > (\log f)/4$, by the preceding lemmas. For a quartic field, (26.6) gives this when $\log f \geq 16$, since $\sqrt{10}/4 < 4/5$ and $\log 16 < 3$. If $f = p$ then $f_2 = p$. For

$p \geq 64$ we have $(3/2)\log p - \log 16 \geq (5/6)\log p > (\sqrt{10}/4)\log p$. In degree six, add the three inequalities in (26.7) with weights $1, 2, 3$. Both proper conductors cancel. This gives

$$6 \log f \leq \log(216 \cdot 4^2 \cdot 8^3) + (\sqrt{208/3} + 8 + 4\sqrt{3})\sqrt{Q}.$$

The constant is less than 15 and the coefficient is less than $70/3$. If $\log f \geq 90$, then $15 \leq (\log f)/6$. The desired strict inequality follows.

Suppose now $m = 6$ and $f = p$ is prime. The unique prime above p is totally ramified with residue field $\mathbf{F}_p$. All conjugates of z therefore have the same residue a. Its norms to k_2, k_3 are signs, so $a^6 = a^4 = 1$. Change the sign of z to arrange $a = 1$. Both norms are then $+1$, as p is odd. Each pair over k_3 consists of actual reciprocals. The conjugates with indices $0, 2, 4$ are representatives of the three reciprocal pairs and their product is one. At most two representatives are negative.

The nonzero integer $|N_{F/\mathbb{Q}}(1 - z)|$ is divisible by p. For a reciprocal pair x, x^{-1}, put $L = |\log|x||$. Its contribution to this integer is $e^L(1 - e^{-L})^2$ for $x > 0$, and $e^L(1 + e^{-L})^2$ for $x < 0$. Multiplication over the three pairs gives

$$p \leq 16e^{2(A+B)} \leq 16e^{4\sqrt{Q/3}}.$$

If $p \geq 2^{10}$, then $\log p - \log 16 \geq (3/5)\log p$ and $3\sqrt{3}/5 > 1$. This gives $\sqrt{Q} > (\log p)/4$. □

Theorem 26.11 (Prime conductor at every layer)**.** *Let p be an odd prime and let F be any subfield of $\mathbb{Q}(\zeta_p)^+$ of degree $m \in \{1, 2, 3, 4, 6\}$. Let $\mathbb{Q}_n$ be the field of degree p^n in $\mathbb{Q}(\zeta_{p^{n+1}})$. Then $p \nmid h(F\mathbb{Q}_n)$ for every $n \geq 0$.*

Proof. Begin at $n = 0$. The case $m = 1$ is immediate. For the quadratic field its discriminant is p and each ideal class has an integral representative of norm at most $Y = \sqrt{p}/2$ by Minkowski's theorem. At most $\sum_{ab \leq Y} 1 \leq Y^2 < p$ such ideals exist, because at a rational prime power q^j there are at most $j + 1$ choices. In the cubic case the claim follows from Lemma 24.22 with $f = p$. In degrees four and six the proper subfields therefore have class numbers prime to p. Proposition 26.10 proves the claim above its prime-conductor thresholds.

Here is an exact check below the thresholds. Such a real subfield exists precisely when $2m \mid p - 1$. Let $L = \mathbb{Q}(\zeta_p)$ and let ω be its mod-p cyclotomic character. The two faithful characters of F on $\mathbf{F}_p$ lift to ω^k and ω^{p-1-k} on $\mathrm{Gal}(L/\mathbb{Q})$, where $k = (p-1)/m$. If $\mathrm{Cl}(F)/p\,\mathrm{Cl}(F)$ were nonzero, a faithful character would occur. Indeed every nonfaithful summand is invariant under the subgroup defining a proper subfield. Its group sum is extension of the ideal norm, and acts on invariants by the subgroup order, a unit modulo p. The preceding proper-subfield conclusion rules this out. The same norm and extension identities show that a nonzero faithful summand would persist in $\mathrm{Cl}(L)/p\,\mathrm{Cl}(L)$.

For either exponent $u \in \{k, p-1-k\}$, suppose such a summand exists. The group $\mathrm{Gal}(L/\mathbb{Q})$ has order $p-1$, so there is a nonzero equivariant homomorphism from $\mathrm{Cl}(L)$ to $\mathbf{F}_p(\omega^u)$. It gives an unramified homomorphism on G_L by class field theory. Its restriction at the prime above p is zero since that prime is generated by $1-\zeta_p$. After identifying its values with μ_p, Kummer theory gives a nonzero class of character $\beta = \omega^{1-u}$ in $L^\times/L^{\times p}$. Conjugation on values contributes ω and precomposition with inverse conjugation contributes ω^{-u}. Its valuations are multiples of p. Indeed the class is trivial at p, and at each other finite place it becomes trivial over the maximal unramified extension, which preserves the value group. Thus, writing $(y) = \mathfrak{a}^p$, it maps to $[\mathfrak{a}] \in \mathrm{Cl}(L)[p]$. The kernel consists of unit classes. Their odd part is generated by roots of unity. Indeed, for any unit v, the quotient $v/\bar{v}$ has absolute value one under every embedding and is a root of unity. Since p is odd, the operator $1 - c$ spans the odd part, where

c is complex conjugation. The character on its roots of unity modulo p-th powers is ω. But u is even and $u \not\equiv 0 \pmod{p-1}$, so β is odd and differs from ω. Our image in $\mathrm{Cl}(L)[p]$ is therefore nonzero.

For $p \nmid b$, the integral Stickelberger element $(b - \sigma_b)\Theta_p$ annihilates this image. Its action on the β-component is multiplication by

$$T_b(u) = \sum_{j=1}^{p-1} \left\lfloor \frac{bj}{p} \right\rfloor j^{u-1} \pmod{p}, \tag{26.8}$$

since the coefficient of σ_j^{-1} in this element is $\lfloor bj/p \rfloor$ and $\beta(j)^{-1} = j^{u-1}$. This is also the group-ring computation in Theorem 24.3. [1, Ch. 6] It suffices to exhibit a nonzero value for each u.

For degree four the two rows $(p, b, T_b(k), T_b(p-1-k))$ are $(17, 2, 13, 7)$ and $(41, 2, 5, 29)$. For degree six the table gives the two residues in that order. A superscript star uses $b = 3$, and every other entry uses $b = 2$.

p	$T_b(k)$	$T_b(p-1-k)$	p	$T_b(k)$	$T_b(p-1-k)$	p	$T_b(k)$	$T_b(p-1-k)$
13	5	10	337	12	128	673	545	222
37	24	36	349	169	240	709	449	512
61	34	27	373	190	214	733	495	393
73	40	63	397	184	275	757	539	455
97	94	56	409	367	200	769	465	734
109	10	90	421	192	301	829	109	85
157	86	18	433*	82	387	853	779	180
181	133	104	457*	367	312	877	449	270
193	80	54	541	184	274	937	467	284
229	78	108	577	323	364	997	587	991
241	134	196	601*	242	65	1009	610	546
277	122	26	613	229	139	1021	388	291
313	155	92	661	615	221			

For reproducibility, enumerate $p = 1 + 2ma$ below the relevant threshold, starting with $a = 1$. Discard candidates divisible by a prime at most $\sqrt{p}$. To verify each table entry using only integer arithmetic, initialize $T = 0$ and for $j = 1, \dots, p-1$ compute $j^{u-1} \bmod p$ by repeated squaring. Add its product with the integer quotient of bj by p to T, reducing modulo p at each step. For example at $m = 6, p = 13, k = 2, b = 2$ the first residue is $7 + 8 + 9 + 10 + 11 + 12 \equiv 5 \pmod{13}$. All residues are nonzero, proving the claim at the base.

It remains to pass up the tower. At each step $L_1 = F\mathbb{Q}_{n+1}$ over $L_0 = F\mathbb{Q}_n$, the extension is cyclic of degree p. Only the unique prime above p ramifies, and it is totally ramified. These facts follow by restriction from the prime-power cyclotomic field, since $[F : \mathbb{Q}]$ is prime to p. Suppose $p \nmid h_{L_0}$ and let B be the maximal unramified elementary abelian p-extension of L_1 split at its real places. It is Galois over L_0 by uniqueness, and $G = \mathrm{Gal}(B/L_0)$ is a finite p-group. The inertia subgroup above p has order p, because B/L_1 is unramified. Its normal closure is all of G, since the quotient defines an everywhere unramified extension of L_0, split at the real places, and a nontrivial finite p-group quotient would have a cyclic quotient of order p. Class field theory excludes this by $p \nmid h_{L_0}$. Every maximal subgroup of a finite p-group is normal. The inertia group therefore cannot be proper, since it would be contained in a maximal subgroup. Thus $|G| = p$, giving $B = L_1$ and $p \nmid h_{L_1}$. Induction proves the theorem. □

Corollary 26.12 (Strict groups of residual order four or six)**.** *In Theorem 24.20, let the even residual character τ cut out a field F of degree $m = 4$ or 6. Suppose the coefficient prime p does not split completely in F. If $p^{\mathrm{ord}_m(p)} > H$, then $S(\vartheta) = 0$. Vanishing holds whenever $f = p$.*

For arbitrary conductor it also holds if $p^{\mathrm{ord}_m(p)} \geq f$ *and* $\log f \geq 16$ *for* $m = 4$ *or* $\log f \geq 90$ *for* $m = 6$.

Proof. The order m of the residual character is prime to p. Since it is faithful on $\mathrm{Gal}(F/\mathbb{Q})$, the nonsplitting assumption makes it nontrivial on a decomposition group at p. By Theorem 24.20, the elements of $S(\vartheta)$ killed by p are dual to the τ-part of the ordinary class group modulo p after extension of residue scalars. Indeed the classes of the primes above p have zero image on this character, since their stabilizers act nontrivially on it. A nonzero such part requires a faithful irreducible constituent over $\mathbf{F}_p$. Lemma 26.8 and Proposition 26.10 give the stated tests for arbitrary conductor. Theorem 26.11 treats every prime conductor equal to the coefficient prime. Finally a nonzero p-primary torsion group contains an element of order p, so the first-layer vanishing gives vanishing at every exponent. □

26.4 Norms of ideal classes in the remaining cohomology estimate

Fix x in the same interval as in (19.15) and keep the field $E = K_\psi C_J(\sqrt{-q}, \sqrt{-d_0})$ used for the theta comparison. For an odd prime p, let K be the maximal subfield of E of p-power degree, $p^a = [K : \mathbb{Q}]$. Let $\mathbb{Q}_i$ be the degree-p^i layer of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, and set

$$L = (E(\mu_p))^+, \quad p^d = [K \cap \mathbb{Q}_\infty : \mathbb{Q}], \quad L_i = L\mathbb{Q}_{d+i}, \quad A_i = \mathrm{Cl}(\mathcal{O}_{L_i}[1/p])\{p\}.$$

For a character α of the prime-to-p part of $\mathrm{Gal}(E/\mathbb{Q})$, extended trivially over the p-part, consider its complementary twists $\alpha(c) = (-1)^r$. Write $\tau = \alpha^{-1}\omega^{-r}$ on G_K, with ω the Teichmüller character. With coefficients in a splitting unramified ring O of residue field $\mathbf{f}$, put $C_i = e_\tau(A_i \otimes O)$, and let $S_\alpha = e_\alpha(M_{p,r} \otimes O)$. One tower of fields works for all these characters and twists at this p.

Theorem 26.13 (Class-group growth forced by a surviving strict class)**.** *Write* $k = k_{p,r}$, $h = 1 + d + v_p(r)$, $n_0 = a - d$, *and* $D = \dim_{\mathbf{f}}(p^k S_\alpha)[p]$. *When* $k \geq h + n_0$, *for every* $n_0 \leq n \leq k - h$ *one has*

$$\dim_{\mathbf{f}} \frac{\ker(C_{n+1} \to C_n)}{(p, \gamma - 1)\ker(C_{n+1} \to C_n)} \geq D,$$

where γ *generates* $\mathrm{Gal}(L\mathbb{Q}_\infty/L)$ *and the maps are norms. In particular*

$$\log \frac{|C_{k-h+1}|}{|C_{n_0}|} \geq (k - h - n_0 + 1)D \log |\mathbf{f}|. \tag{26.9}$$

If one of these transitions has equal class-group orders, this entire character contributes zero beyond depth k *in* (19.15). *The assertion applies at primes dividing the degree of the period field as well.*

Proof. Restriction to E/K and averaging over its prime-to-p Galois group identify S_α with the strict cohomology of $\alpha^{-1}\kappa_p^{-r}$ over K. Over $L\mathbb{Q}_\infty$ this character becomes trivial. Its strict classes are dual to the quotients of the C_m by $\gamma - (1 + p)^{-rp^d}$ as m grows. Local restriction in this descent is injective even at split primes above p because the principal cyclotomic image is open and multiplication by a nonzero power of its generator minus one is surjective on the divisible coefficient group. The complete argument is in Lemma 26.1.

For $m > n \geq n_0$, total ramification implies that the kernel of $C_m \to C_{n+1}$ is the image of the kernel of $C_m \to C_n$ under $1 + \gamma^{p^n} + \cdots + \gamma^{(p-1)p^n}$. This operator belongs to $(p, \gamma - 1)$. In the specialization for the twist, $\gamma^{p^n} - 1$ is a unit times p^{h+n}. Consequently the rank on the left bounds the number of elementary divisors of S_α with exponent greater than $h + n$, as proved in

Lemmas 26.1–26.2 and Theorem 26.3. At $h+n \le k$ this includes all D summands of exponent greater than k. The norms are surjective, so summing the logarithms of their kernel orders gives (26.9). Equal orders at any indicated step force $D = 0$, and then $p^k S_\alpha = 0$ by finiteness. This also kills its contribution after the projector used in (19.15). □

For $p \le b^{1/12}$, the lower bound on $k_{p,r}$ in Theorem 19.19 tends to infinity uniformly faster than $\log(2x)$. Here $a \le v_p(\operatorname{ord}\psi)$ and $v_p(r) \le \log_p t$. Hence every surviving component in this range forces growth at every one of the indicated consecutive layers. At the larger primes the same test applies whenever $k \ge h + n_0$.

Corollary 26.14 (Exact lengths for two primitive characters)**.** *On every period field for the primitive quadratic character of discriminant* 268*, its own complementary component at* 3 *has order three for every positive even twist. For the character of discriminant* -804 *the corresponding statement holds for every positive odd twist.*

Proof. In both cases $\alpha = \psi$ and $\psi^{-1}\omega^{-r} = \chi_{268}$. On the cyclotomic $\mathbb{Z}_3$-tower of $\mathbb{Q}(\sqrt{67})$ the class group modulo the primes above 3 has 3-part of order three from layer three onward. Fukuda and Komatsu's quadratic-field theorem gives this index. The verification of its numerical hypotheses, the character action and descent to the original period field is in Proposition 26.4 and Theorem 26.5. The pro-3 action on the limiting cyclic group and the twisting character modulo three are both trivial. Its twisted dual therefore still has order three. In particular the contribution of this component to the original sum is exactly $\log 3$ at each indicated twist. □

To obtain the cohomological bound in Section 6.6 one still needs an upper estimate for the total orders of the surviving components in (19.15). Equation (26.9) gives a necessary growth condition for them. The required lower arithmetic comparison for the integral theta period at its original finite level also remains open in this manuscript.

26.5 A bound for all twists from two fields at each prime

Use the cyclotomic tower and norm groups of Theorem 26.13. The residual character determines which twists must be treated together. Polynomial interpolation in the cyclotomic generator gives the following simultaneous bound.

Theorem 26.15 (A simultaneous estimate for the remaining classes)**.** *Put* $\bar{k}_{p,r} = \max(1, k_{p,r})$ *and* $n_0 = a - d$*. For all sufficiently large* x *on the same intervals, for each odd prime* p*, and for every* $j \ge 1$*, one has*

$$\sum_{1 \le r < t} \log \left| (p^{\bar{k}_{p,r}} M_{p,r})[p^j] \right| \;\le\; \log \left| \ker(A_{n_0+j} \longrightarrow A_{n_0}) \right|. \tag{26.10}$$

The groups on the right are p*-parts of ideal class groups with all primes above* p *divided out. In particular the number of cyclic summands surviving these depths, summed over every twist, is at most the base-*p *logarithm of the first norm kernel (*$j = 1$*). If the right side for any* j *is strictly less than* $j \log p$*, it bounds the sum of the full orders in logarithmic scale at this prime.*

Proof. For a fixed residual character write $u_r = (1+p)^{-rp^d}$. At a common finite level m all the strict groups in this character are dual to the quotients by $\gamma - u_r$ of the same class-group component. Multiplying a lift of a class in the r-th quotient by $(\gamma^{p^{n_0}} - 1)\prod_{s \ne r}(\gamma - u_s)$ kills its other coordinates and puts it in the norm kernel down to n_0. The product ranges over the other twists in that residual character. Its loss, including the first factor, is at most $\bar{k}_{p,r}$. For $p \le \exp(x^{\varepsilon}/12)$ this follows from the factorial bound for the valuations of the distinct $r - s$ and Theorem 19.19. For larger p the twists are distinct on inertia and the loss is one.

In these independent coordinates the sum of the first p^j powers of $\gamma^{p^{n_0}}$ acts by a scalar of valuation j on each coordinate. Its kernel therefore contains the pieces killed by p^j in (26.10). Its cokernel on the joint image is a quotient of the norm kernel from $n_0 + j$ to n_0. Kernel and cokernel have equal sizes on the finite image. Summing over the disjoint residual characters and descending the unramified coefficients gives the inequality. The joint image, the exact norm relation and the full valuation bound are proved in Theorem 26.6 and Corollary 26.7. Finally an elementary divisor of a surviving group of order at least p^j would contribute at least $j \log p$ to the left side. This proves the last assertion. □

When $k_{p,r} = 0$, the term of (19.15) also uses the first layer of $Q_{p,r}$. Its exact contribution at that layer is $\log |Q_{p,r}[p]|$. At every other depth (26.10) applies directly to the tails in (19.15) because $Q_{p,r}$ is a summand of $M_{p,r}$. The estimate required for Dirichlet GRH concerns full orders summed over the coefficient primes. The explicit class-number bound in Corollary 26.7 increases with j and does not supply that estimate.

In the accompanying source, `Development/AutomorphicArithmetic/AutomorphicVarieties/HeightAndVanishing/Counts.lean`, line 53 states one of the bounds needed for full orders. For its first case it sums over characters and over any finite set of allowed coefficient primes, at fixed twist $r < t$, with upper bound $(Nt)^C$. The proof in `Development/AutomorphicArithmetic/AutomorphicVarieties/ModularityArgument/ThresholdArguments/DenseThresholdCases/LinkedUnlE.lean`, line 49 uses a cohomology estimate, rigidity and automorphy inputs. Equation (26.10) proves a finite-layer estimate by class field theory. A uniform bound for the full global sum and the lower arithmetic comparison for the designated integral theta period remain the two outstanding steps of Section 6.6.

26.6 Vanishing at quartic and sextic residual characters

We first consider the classes descending from $\mathbb{Q}$. In the rational summand of the cohomological estimate the same twist r must be treated at many coefficient primes p. Two additional families can be removed at every exponent.

Theorem 26.16 (The rational summand for characters of orders four and six)**.** *For every positive even integer r and every odd prime p,*

$$p - 1 \mid 4r \quad \text{or} \quad p - 1 \mid 6r \qquad \Longrightarrow \qquad K_{2r}(\mathbb{Z})\{p\} = 0.$$

Consequently the supremum in (20.5) is unchanged when its finite prime sets are restricted to primes $p \geq 5$ satisfying both $p - 1 \nmid 4r$ and $p - 1 \nmid 6r$.

Proof. Put $D = \mathbb{Q}(\zeta_p)^+$. By Proposition 11.19, the dimension of $K_{2r}(\mathbb{Z})/p$ is the dimension of the ω^{-r}-part of $\mathrm{Cl}(D)/p$, where ω describes the action on μ_p. The character is even. Its order is $m = (p-1)/\gcd(p-1, r)$, so our two divisibility conditions give precisely $m \in \{1, 2, 3, 4, 6\}$. Let F be the field cut out by this character. Extension and norm of ideal classes identify $\mathrm{Cl}(F)/p$ with the invariants in $\mathrm{Cl}(D)/p$ under $\mathrm{Gal}(D/F)$. Indeed their two composites are multiplication by $[D : F]$ and the subgroup sum, respectively, and the degree is a unit modulo p. The desired eigenspace belongs to these invariants.

The class number of every such F is prime to p. For degrees four and six one divides the analytic class number formula for F by the formulas for its proper subfields. Only two primitive Dirichlet values remain. Relative units bound the quotient of the regulators from below and give a class number quotient less than p above explicit thresholds. For the smaller primes the two faithful characters are excluded by exact nonzero Stickelberger residues. The calculation, including all coefficients in the regulator bounds and the small primes, is proved in Lemmas

26.8–26.9, Proposition 26.10 and Theorem 26.11. The latter theorem also treats degrees one, two and three. Thus the eigenspace is zero and finiteness of $K_{2r}(\mathbb{Z})$ gives vanishing at every exponent. Proposition 20.6 identifies the orders in its supremum with the corresponding primary orders, so deleting the zero terms preserves the equality. □

Corollary 26.17 (Character components on the theta fields)**.** *Fix an admissible x, its field E in (19.15), an odd prime $p \nmid [E:\mathbb{Q}]$, and $1 \le r < t(x)$. Extend coefficients to an unramified ring containing the values of the characters of $\mathrm{Gal}(E/\mathbb{Q})$. The trivial character summand of $M_{p,r}$ is zero for the even twists and primes of Theorem 26.16.*

More generally, let $\alpha(c) = (-1)^r$ and suppose the even residual character $\tau = \overline{\kappa_p^{-r}\alpha^{-1}}$ has order $m = 4$ or 6. Let F be its field and f its conductor. Assume that p does not split completely in F. The α-component of $M_{p,r}$ vanishes if $f = p$. It also vanishes if $p^{\mathrm{ord}_m(p)} \ge f$ and $\log f \ge 16$ in degree four or $\log f \ge 90$ in degree six.

Proof. Averaging over the prime-to-p group $\mathrm{Gal}(E/\mathbb{Q})$ identifies the character summand with the strict group over $\mathbb{Q}$ for the coefficient $(J/O)(\kappa_p^{-r}\alpha^{-1})$, where O is the chosen coefficient ring and J is its fraction field. The same averaging on inertia away from p and on decomposition groups at p preserves the strict local conditions, as proved in Theorem 24.1. For $\alpha = 1$ and r even, its Pontryagin dual over $\mathbb{Z}_p$ before extending scalars is $K_{2r}(\mathbb{Z})\{p\}$, by Proposition 11.19 and its proof.

In the second assertion, the finite coefficient lift of an order-p class is locally zero at p, because some local element acts by $\tau(g) \ne 1$ modulo p. Restricting to F makes the residual coefficient trivial. Class field theory therefore identifies these classes with homomorphisms on the faithful component of the ordinary class group modulo p. Classes of primes over p are killed automatically on this component by their stabilizers. The norm-kernel and prime-conductor bounds give its vanishing under the indicated conditions, by Corollary 26.12. A nonzero primary torsion group has an element of order p. This proves vanishing of the entire component on the original field for each indicated x. □

In the supplied source, `Development/AutomorphicArithmetic/AutomorphicVarieties/HeightAndVanishing/Counts.lean`, line 49 uses a rational vanishing statement for $p-1 \mid 2r$. The two results above extend the range of such vanishing. The other residual characters still occur in the sum. At a prime $p > 6t+1$, all positive even twists $r < t$ already have order greater than six on the rational summand, since $(p-1)/\gcd(p-1,r) \ge (p-1)/r > 6$. The uniform total in (19.15) and the lower arithmetic estimate for the original finite-level integral theta period are still needed on the common intervals.

26.7 A bound in every twist on a cyclic sextic subfield

Theorem 26.18 (A uniform positive contribution when three divides the degree)**.** *Let $B = \mathbb{Q}(\zeta_7)^+$, $K = \mathbb{Q}(\sqrt{257})$ and $F = BK$. For each positive even r, the order of the actual strict group $\mathcal{S}_{3,r}(F)$ is either 3 or 9. It depends only on $r \bmod 6$. For any character cutting out F, put $h_x = \lfloor (t(x)-1)/2 \rfloor$. On its original interval fields one has*

$$h_x \log 3 \;\le\; \sum_{1 \le r < t(x)} \log \left| \left(\mathcal{S}_{3,r}(E_x)^{c=(-1)^r}\right)^{\mathrm{Gal}(E_x/F)} \right| \;\le\; h_x \log 9.$$

Proof. The prime 3 is inert in B, since 3 generates $(\mathbb{Z}/7)^\times$. Theorem 27.5 gives $\mathcal{S}_{3,r}(B) = 0$ at every even twist. The other summand under the involution of F/B is $S(B,A)$ with $A = (\mathbb{Q}_3/\mathbb{Z}_3)(\chi\kappa_3^{-r})$ for the quadratic character χ of conductor 257. Quadratic descent applies integrally at 3. Here $\chi(3) = \chi(7) = -1$. For example the 128-th powers of 3 and 7 are both

$-1 \bmod 257$. Thus Theorem 19.24 applies with $p = 3$, $a = 1$, $b = 7$. It identifies the lengths of the two character quotients with d_0, d_1 and bounds the length on the cubic field between their maximum and their sum. Theorem 27.8 gives $d_0 = 1$.

For d_1, take the cubic character λ modulo 7 with $\lambda(3) = \zeta_3$. Put $\pi = \zeta_3 - 1$, so that $\pi^2 = -3(1 + \pi)$. In $\mathbb{Z}_3[\zeta_3]/3$ one has $\zeta_3^j = 1 + j\pi$, and $\pi \neq 0$. The reduction argument in Theorem 19.24 gives $d_1 \geq 1$. For the reverse bound evaluate the class at $s = 43177 = 8{\cdot}5397{+}1$, where $5397 = 257 \cdot 7 \cdot 3$. Trial division through 207 proves primality. Take $g = 5$ and $w = g^8 = 2032 \bmod s$. For $d = 2, 3, 7, 257$, the residues $g^{(s-1)/d}$ are $43176, 15074, 18105, 21688$. This checks that g is a generator. For $1 \leq a < 5397$ prime to 5397, write $a = 3^{j(a)} \bmod 7$, with $j(a)$ taken modulo three after computing the logarithm modulo six. Form the three sums

$$C_j = \sum_{j(a)=j} \chi(a) \operatorname{ind}_g(1 - w^a) \bmod 3, \qquad (C_0, C_1, C_2) = (0, 2, 1).$$

To reproduce them, advance y from 1 by multiplying by $w \bmod s$ for each integer $a = 1, \ldots, 5396$. Retain the terms prime to 5397. The index modulo three is the unique $i \in \{0, 1, 2\}$ such that $(1 - y)^{(s-1)/3} = w^{1799i} \bmod s$. Give it sign $+1$ or -1 according as a^{128} is 1 or $-1 \bmod 257$. The successive residues of $3^j \bmod 7$ for $j = 0, \ldots, 5$ are $1, 3, 2, 6, 4, 5$, which assigns the entry.

For every positive even r, the twist factor a^r is one modulo three. Proposition 21.10 therefore evaluates the corestricted class, up to a unit, as $\sum_j C_j(1 + j\pi) = \pi \bmod \pi^2$. Thus $d_1 = 1$. This proves both bounds on the actual group over F. As its exponent divides nine, it equals its nine-torsion. Lemma 24.11 identifies the nine-torsion at any two positive twists congruent modulo six. Equivalently, at these twists the finite coefficient actions agree modulo nine and the local cyclotomic kernels in that lemma agree as well. This proves the asserted periodicity. Finally $[E_x : F]$ is a power of two on the fields of Theorem 19.15. Restriction gives the same invariant group there. The sign on the real field F excludes the odd twists and counting the even twists gives the two inequalities. □

These results evaluate part of the cohomology sum on the fields used for the theta period. The sum over the other components and the upper and lower estimates for the normalized integral period in Section 6.6 remain open.

26.8 The full strict groups over the cyclic sextic field

Theorem 26.19 (Exact cyclic groups at all positive even twists)**.** *Let $F = \mathbb{Q}(\sqrt{257}, \zeta_7 + \zeta_7^{-1})$. Then*

$$\mathcal{S}_{3,r}(F) \simeq \begin{cases} \mathbb{Z}/9\mathbb{Z}, & r \equiv 0 \pmod 6,\ r > 0, \\ \mathbb{Z}/3\mathbb{Z}, & r \equiv 2, 4 \pmod 6,\ r > 0. \end{cases}$$

For any Dirichlet character cutting out F, put $t = \lfloor x^{401} \rfloor$. At every point on the common intervals the invariant contribution on its original fields E_x is

$$\sum_{r=1}^{t-1} \log \left| (\mathcal{S}_{3,r}(E_x)^{c=(-1)^r})^{\mathrm{Gal}(E_x/F)} \right| = \left(\left\lfloor \frac{t-1}{2} \right\rfloor + \left\lfloor \frac{t-1}{6} \right\rfloor \right) \log 3.$$

Proof. Keep the quadratic character χ, the cubic character λ and the open set U of Proposition 27.6. Both integral character lattices have degree-two length one. All the local invariant terms vanish in their quadratic character sector at $3, 7, 257$, as proved in Theorem 19.24. The sector for the trivial quadratic character contributes zero by Theorem 27.5 for $\mathbb{Q}(\zeta_7)^+$. Thus the integral degree-two group for

$$T_R = \mathbb{Z}_3(\chi\kappa_3^{r+1}) \otimes R, \qquad R = \mathbb{Z}_3[X]/(X^3 - 1),$$

is dual to the entire strict group over F, by Shapiro's lemma and the duality sequence of Theorem 9.4. For the integral group ring the dual lattice agrees with the regular lattice, since the basis of group elements is orthonormal for its invariant pairing. By Theorem 19.25 the length is $1+1-1+\dim(L_0\cap L_1)$. The proposition therefore gives length two when $6\mid r$ and one for the other positive even twists.

To determine the abelian group, put $M=H^2(U,T_R)$ and $\Phi=X^2+X+1$. One has $M/\Phi M=H^2(U,T_R/\Phi T_R)$. Indeed degree two is the last cohomological degree. Applying the long exact sequence first to the image of multiplication by Φ, and then to its inclusion, shows that its image on cohomology is ΦM and that the displayed quotient map is surjective. The lattice quotient is the one for $\chi\lambda$, whose degree-two group has order three. Consequently, for $\bar M=M/3M$ and $Y=X-1$, one has $\dim_{\mathbb{F}_3}\bar M/Y^2\bar M=1$, since $\Phi=Y^2 \bmod 3$. Now $Y^3=0$ on $\bar M$. Its nonzero quotient modulo Y^2 therefore has nonzero quotient modulo Y. Both quotients have dimension one, so $Y\bar M=Y^2\bar M$, and nilpotence gives $Y\bar M=0$. It follows that $\bar M$ has dimension one. The finite abelian 3-group M, and hence its dual, is cyclic. This proves the asserted isomorphism in each weight.

Finally $[E_x:F]$ is a power of two and restriction identifies the strict group with the invariant part as in Theorem 26.18. The complementary part at an odd weight vanishes on the real field F. Each even weight contributes $\log 3$, with a second $\log 3$ at each positive multiple of six. Counting them gives the equality. □

The full interval estimate also includes the other characters of E_x and the other coefficient primes. Their total and the two estimates for the prescribed integral theta period in Section 6.6 remain to be proved.

26.9 Two infinite families of character fields with exact strict orders

Keep $K=\mathbb{Q}(\sqrt{257})$, F, L and γ of Theorem 27.7. Let τ be either generator of $\mathrm{Gal}(F/K)$, extended to fix Q_∞. For $m\ge 2$ and $e\in\{1,-1\}$ define $D_{m,e}$ as the fixed field in L of the closed subgroup generated by $\delta=\tau^e\gamma^{3^{m-1}}$. Let $D^+_{m,e}=D_{m,e}$, let $B_{m,e}$ be its degree-3^m subfield, and put $D^-_{m,e}=B_{m,e}\mathbb{Q}(\sqrt{-771})$.

Theorem 26.20 (Exact orders for character fields of unbounded conductor)**.** *Each $D^{\pm}_{m,e}$ is cyclic of degree $2\cdot 3^m$ over $\mathbb{Q}$ and has conductor $257\cdot 7\cdot 3^{m+1}$. At every positive twist the complementary strict group is given by*

$\mathcal{S}_{3,r}(D)^{c=(-1)^r}$	r even	r odd
$D=D^+_{m,e}$	$\mathbb{Z}/3\mathbb{Z}$	0
$D=D^-_{m,e}$	0	$\mathbb{Z}/3\mathbb{Z}$

In particular, for any primitive Dirichlet character cutting out one of these fields D, at every point of the original common intervals,

$$\sum_{1\le r<t(x)}\log\left|\left(\mathcal{S}_{3,r}(E_x)^{c=(-1)^r}\right)^{\mathrm{Gal}(E_x/D)}\right|=\begin{cases}\lfloor (t(x)-1)/2\rfloor\log 3, & D=D^+_{m,e},\\ \lfloor t(x)/2\rfloor\log 3, & D=D^-_{m,e}.\end{cases}$$

Proof. The Galois group of $L/\mathbb{Q}$ is the product of the quadratic group of K, the cubic group generated by τ, and Γ generated topologically by γ. In the last two factors the quotient by δ is generated by the image of γ, since $\tau^e=\gamma^{-3^{m-1}}$ there. It has exact order 3^m, because the intersection of the closed subgroup generated by δ with Γ is generated by $\delta^3=\gamma^{3^m}$. The quadratic factor is independent, so $D_{m,e}$ has the asserted cyclic Galois group. The two signs give distinct subgroups, since they give different cubic components above $\gamma^{3^{m-1}}$.

For the conductor, choose the character on Γ with value ζ_{3^m} on γ, taken trivial on the Teichmüller factor. Its conductor is 3^{m+1}, since the order of 4 mod 3^{m+1} is 3^m and the preceding modulus gives order 3^{m-1}. Multiply this character by the cubic character taking τ to ζ_3^{-e} and the quadratic character of conductor 257, choosing $\zeta_{3^m}^{3^{m-1}} = \zeta_3$. The product kills δ and has order $2 \cdot 3^m$, so it cuts out $D_{m,e}$. The three primitive factors have pairwise coprime conductors. Each retains its conductor on its own inertia group, giving the product conductor. Multiplication by the quadratic character ω of $\mathbb{Q}(\sqrt{-3})$ replaces the quadratic factor by that of $\mathbb{Q}(\sqrt{-771})$. The 3-part of the product character's conductor is still 3^{m+1}, since ω is trivial on principal units and the character on Γ is primitive there. This proves the statements on the degree and conductor for the imaginary fields as well.

The extension $L/D_{m,e}$ has group $\mathbb{Z}_3$ generated by δ, as follows by projection to Γ. Outside 3 the only possible ramification of $L/\mathbb{Q}$ is at 7 and 257, whose inertia groups are finite and meet this torsion-free subgroup trivially. Thus the twisted quotient in Theorem 27.7 applies. By Theorem 27.9, X is cyclic of order nine, γ acts trivially, and τ acts by a unit of order three in $(\mathbb{Z}/9)^\times$. Such a unit is 4 or 7, so subtracting one gives a multiple of three of valuation exactly one. Since $m \geq 2$, $u(\delta)^{-r} = 4^{-3^{m-1}r} \equiv 1 \bmod 9$. The twisted quotient $S(D_{m,e}^+, A_r^{\mathrm{pr}})$ is consequently cyclic of order three for either e and every $r \geq 1$. The quadratic involution σ acts on this group by -1 by Theorem 27.9. Indeed it fixes Q_∞, hence acts trivially on the coefficient in the equivariant homomorphisms of Theorem 27.7.

Write $B = B_{m,e}$. Quadratic descent from $D_{m,e}^+ = BK$ therefore gives $S(B, A_r^{\mathrm{pr}}) = 0$ and $S(B, A_r^{\mathrm{pr}} \otimes \chi_{257}) \simeq \mathbb{Z}/3\mathbb{Z}$, where χ_{257} is the character of K. Here the two summands arise by applying the two integral quadratic projectors to the induced coefficient. Restriction detects unramifiedness on inertia and the zero local class at three since all relative local degrees divide two. On the real field $D_{m,e}^+$ the even twist uses A_r^{pr}, and the odd complementary sign is absent. On $D_{m,e}^-/B$ complex conjugation is the nontrivial quadratic automorphism with character $\chi_{257}\omega$. At an even twist its plus summand is $S(B, A_r^{\mathrm{pr}})$. At an odd twist its minus summand has coefficient character $\kappa_3^{-r}\chi_{257}\omega = \langle\kappa_3\rangle^{-r}\chi_{257}$. This gives both rows of the table.

Finally the relative degree $[E_x : D]$ for these characters is a power of two. Restriction and averaging preserve the global and local conditions, as in Theorem 27.5. Counting the positive even or odd twists less than $t(x)$ now gives the two formulas. □

The calculation follows the indicated invariant part as the conductor grows. The other parts of the strict groups on E_x and the required integral theta-period estimates in Section 6.6 remain open.

26.10 Exact strict groups for cyclic fields with several ramified primes

Let p be an odd prime and $b_1, \dots, b_m$ distinct primes congruent to 1 mod p, where $m \geq 1$. Choose surjections $\nu_i : (\mathbb{Z}/b_i\mathbb{Z})^\times \to (\mathbb{F}_p, +)$. They define a Dirichlet character $\psi = \zeta_p^{\sum_i \nu_i}$. Its field K is cyclic of degree p, is totally real and has conductor $\prod_i b_i$, since each local component has order p. Define a matrix over $\mathbb{F}_p$ by

$$D_{ij} = \nu_j(b_i) \quad (i \neq j), \qquad D_{ii} = -\sum_{j \neq i} \nu_j(b_i).$$

We assume that the rational primes satisfy

$$\operatorname{rank} D = m - 1, \qquad \sum_i \nu_i(p) \neq 0.$$

The second says that p is inert in K. The empty minor has determinant one when $m = 1$.

Lemma 26.21 (The strict character groups over the rational field)**.** *Suppose $r > 0$ is a multiple of $p-1$. For every $s \in \mathbb{F}_p$, the strong group $S(\kappa_p^{-r}\psi^{-s})$ over $\mathbb{Q}$ with coefficients in $\mathbb{Q}_p(\zeta_p)/\mathbb{Z}_p[\zeta_p]$ vanishes. Here strictness is imposed at $p, b_1, \dots, b_m$ and classes are unramified elsewhere.*

Proof. Use $\pi = \zeta_p - 1$, so $e = p-1$, and write $\theta_s = \kappa_p^{-r}\psi^{-s}$. Its reduction is trivial. At precision one the global finite characters unramified away from the indicated primes have basis $\nu_0, \nu_1, \dots, \nu_m$. Here ν_0 generates the order-p character group at p of conductor p^2. Indeed Kronecker–Weber identifies these global additive characters with characters of the product of the corresponding cyclotomic factors. At each b_i the higher units are pro-b_i and the residue multiplicative group is cyclic. At p, the p-primary unit factor $1+p\mathbb{Z}_p$ is procyclic and reduction modulo p^2 gives its quotient of order p. There is no infinite-place contribution. Write the coordinates of a character in this basis as $X_0, \dots, X_m$.

First take $s \neq 0$. At p, ψ is unramified with nontrivial value at Frobenius. The cyclotomic part κ_p^{-r} takes values in $1+p\mathbb{Z}_p$, hence is one modulo π^2. It follows that $c_p = 1$ in the notation of Theorem 22.55. The local correcting line at p is unramified and nonzero on Frobenius. Membership in that line gives $X_0 = 0$.

At b_i choose an inertia element of ν_i-value one, and a Frobenius lift with ν_i-value zero. This lift exists by adjustment by inertia and has ν_j-value $\nu_j(b_i)$ for $j \neq i$. Again $c_{b_i} = 1$. On these two elements the correcting character has values $-s$ and $-s\sum_{j\neq i}\nu_j(b_i)$, respectively, since $(\zeta_p^z - 1)/\pi \equiv z \bmod \pi$. A finite character with $X_0 = 0$ has values X_i and $\sum_{j\neq i}\nu_j(b_i)X_j$. In the abelian quotient of exponent p a uniformizer and the cyclic tame unit quotient generate the local group. Proportionality on these two elements therefore gives the entire local condition. For every i it reads

$$\sum_{j\neq i}\nu_j(b_i)(X_j - X_i) = 0.$$

By the rank assumption only the constant vectors survive. These constitute exactly the global correcting line of θ_s, whose m entries are all $-s$. Theorem 22.55 gives zero π-torsion.

If $s = 0$, the local correcting characters at the b_i are unramified, so every X_i, $i \geq 1$, vanishes. The global correcting character generates the remaining line $\mathbb{F}_p\nu_0$. Indeed the cyclotomic image over $\mathbb{Q}$ and its inertia image at p are both $\mathbb{Z}_p^\times$. Thus $(\kappa_p^{-r} - 1)/\pi^{c_\mathbb{Q}}$ is a unit on some element of this inertia group. This again gives zero π-torsion. Each divisible-coefficient cohomology group under consideration is π-primary torsion, so vanishing at precision one proves the lemma. □

Lemma 26.22 (The p-class group detected by the ramified primes)**.** *The p-primary subgroup of $\mathrm{Cl}(K)$ is elementary abelian of rank $m-1$. It is generated by the prime classes above the b_i.*

Proof. Let K' be the compositum of the degree-p fields cut out by the individual ν_i. Their disjoint conductors identify $\mathrm{Gal}(K'/\mathbb{Q})$ with $\mathbb{F}_p^m$, where restriction to K is the sum of the coordinates. Each inertia line in $K'/\mathbb{Q}$ maps injectively to this quotient. Thus K'/K is unramified, including at the real places since all fields are totally real.

Let H_p be the Hilbert p-class field of K and $C = \mathrm{Gal}(H_p/K)$. Global class field theory identifies C equivariantly with $\mathrm{Cl}(K)\{p\}$. The extension $H_p/\mathbb{Q}$ is Galois by the defining maximality. Write σ for a generator of $\mathrm{Gal}(K/\mathbb{Q})$. The commutator subgroup over $\mathbb{Q}$ is $(\sigma - 1)C$, since the group is generated by the abelian normal subgroup C and one lift of σ, and commuting that lift with each member of C gives exactly the claimed subgroup. The maximal subextension abelian over $\mathbb{Q}$ contains K'. It is unramified outside the b_i, with inertia of exponent at most p there since H_p/K is unramified. By Kronecker–Weber its characters are products of local

characters at the b_i of order dividing p, all of which factor through the cyclic residue quotients defining K'. It therefore equals K', and

$$C/(\sigma-1)C \simeq \mathrm{Gal}(K'/K) = \ker\left(\mathbb{F}_p^m \xrightarrow{\sum} \mathbb{F}_p\right).$$

Let $\mathfrak{b}_i$ be the unique prime above b_i in K. Its class is killed by p, since $(b_i) = \mathfrak{b}_i^p$. Its Frobenius in K'/K has coordinates $\nu_j(b_i)$ for $j \neq i$, since its residue degree over $\mathbb{Q}$ is one and those factors are unramified there. Its remaining coordinate is forced by membership in the kernel of the sum. The images of these classes are exactly the rows of D under arithmetic reciprocity. By rank they span $C/(\sigma-1)C$. If B is the subgroup they generate, the finite p-group C/B consequently satisfies $C/B = (\sigma-1)(C/B)$. The operator $\sigma-1$ is nilpotent on this quotient because its p-th power is zero modulo p. Iteration increases divisibility by p until the group is killed. Thus $C = B$. Every generating prime class is fixed by σ, so $C = C/(\sigma-1)C$, as asserted. □

Theorem 26.23 (The complete strict group in the cyclic subfield)**.** *Under the two residue hypotheses, for every positive multiple r of $p-1$ one has*

$$\mathcal{S}_{p,r}(K) \simeq (\mathbb{Z}/p\mathbb{Z})^{m-1}, \qquad \mathcal{S}_{p,r}(E_x)^{\mathrm{Gal}(E_x/K)} \simeq \mathcal{S}_{p,r}(K)$$

on every original period field of ψ.

Proof. Apply the integral Fourier maps in the proof of Theorem 22.57 to $K/\mathbb{Q}$, with strong conditions at p and its conductor. Over K, unramified classes away from p are locally zero in the divisible coefficient by the Frobenius calculation in that proof. All the scalar groups vanish by Lemma 26.21, so multiplication by p kills the original group after extension to $\mathbb{Z}_p[\zeta_p]$. This extension is faithfully flat, hence p kills $\mathcal{S}_{p,r}(K)$ itself.

Compute its p-torsion using $\mathbb{Q}_p/\mathbb{Z}_p$ as coefficient. The mod-p twist is trivial. There is a unique $w \mid p$, and $K_w/\mathbb{Q}_p$ is unramified. The p-power cyclotomic extension of $\mathbb{Q}_p$ is totally ramified, so the local cyclotomic image is $\mathbb{Z}_p^\times$, as is the global image since it contains this local image. In the coefficient sequence for multiplication by p the global correcting line thus restricts isomorphically to the local correcting line at w. In detail, if $c = \min v_p(\kappa_p^{-r} - 1)$, the minimum is the same globally and locally, and the same generator $(\kappa_p^{-r} - 1)/p^c \bmod p$ is nonzero at w. Every strict class therefore has a unique finite-character representative vanishing there, by subtracting its unique global correcting multiple. Away from p the finite character must be unramified, since inertia acts trivially on the divisible coefficient and its connecting image is zero. Conversely, each such everywhere-unramified character split at w represents a strict class. Class field theory gives

$$\mathcal{S}_{p,r}(K)[p] \simeq \mathrm{Hom}\big(\mathrm{Cl}(K)/\langle[w]\rangle, \mathbb{F}_p\big).$$

The prime $w = (p)$ is principal by inertness. The class group lemma and the exponent bound now give the first isomorphism. For the second, the extension E_x/K has degree a power of two. Restriction and averaging identify global classes with the invariants upstairs and detect each local kernel by local restriction, whose degree also divides that power of two. □

For example, take $p = 3$ and $(b_1, b_2, b_3) = (7, 13, 37)$. Take ν_i to be discrete logarithm modulo three to bases $(3, 2, 2)$, respectively. Their powers of exponent $(b_i - 1)/3$ are $2, 3, 26$,

each of order three in its respective residue field. For a residue z, comparison of $z^{(b_i-1)/3}$ with the three powers of this element gives $\nu_i(z)$. This gives $(\nu_i(3)) = (1,1,2)$ and

$$D = \begin{pmatrix} 2 & 2 & 2 \\ 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \quad \text{over } \mathbb{F}_3.$$

The upper left minor is 2, the row sums vanish and the three values at 3 sum to 1 mod 3. Thus on the cyclic cubic field of this character of conductor 3367, the entire strict group has order nine and exponent three at every positive even weight. On its invariant summand in E_x the exact logarithmic contribution for $1 \le r < t(x)$ divisible by $p-1$ is $\lfloor (t(x)-1)/(p-1) \rfloor (m-1)\log p$ in the general theorem. Other character summands on the same fields still enter the estimate in Section 6.6.

26.11 Tame inertia and the strict group in every dyadic layer

Keep the notation $K, P, H, \Delta_H, \chi, M, R_h$ of Theorem 22.58. Assume $\chi(D_p) \neq 1$. Only finitely many primes ramify in the cyclic p-extension $K/\mathbb{Q}$. Among them put

$$T = \{b \neq p : b \text{ ramifies in } K,\ \chi(D_b) = 1\}, \qquad u_b = v_p(e_b(K/\mathbb{Q})), \qquad \mathfrak{m} = \prod_{b \in T} b\mathcal{O}_H.$$

Every $b \in T$ splits completely in H, and $u_b \ge 1$. Use the ordinary ray class group $\mathrm{Cl}_{\mathfrak{m}}(H)$. For $b \in T$ let I_b^{ray} be the image in this group of $\prod_{w \mid b} (\mathcal{O}_H/w)^{\times}$ under the residue-unit map in the ray class sequence. In additive notation put

$$C(K,\chi) = \mathrm{Cl}_{\mathfrak{m}}(H) \Big/ \sum_{b \in T} p^{u_b} I_b^{\mathrm{ray}}.$$

This finite group and its Δ_H-action require only the residual field and the ramification indices of K.

Theorem 26.24 (The ray class group at the split ramified primes)**.** *For $1 \le h \le 1 + v_p(r)$ there is an isomorphism*

$$(M[p^h])^P \simeq \mathrm{Hom}_{\Delta_H}\left(C(K,\chi), R_h(\widetilde{\chi})\right).$$

In particular, $M = 0$ if and only if $\mathrm{Hom}_{\Delta_H}(\mathrm{Cl}_{\mathfrak{m}}(H), k(\chi)) = 0$.

Proof. At the indicated precision the action on R_h is $\widetilde{\chi}$. By Theorem 22.58 and its proof, $M[p^h]$ is the group over K with this coefficient, unramified away from p and locally zero above p. Some value of $\widetilde{\chi} - 1$ at a place over p is a unit, so the coefficient invariants over K vanish. Inflation–restriction identifies the P-fixed global cohomology with first cohomology over $\mathbb{Q}$. We determine the local conditions on that cohomology.

At p, restriction is injective because the same local invariants vanish. At a prime $v \neq p$ unramified in K the inertia group is unchanged. If $v \neq p$ ramifies in K and $\chi(D_v) \neq 1$, its image stays nontrivial on G_{K_w} by the p-power local index. The unramified local cohomology over each of the two fields is zero. Indeed, either inertia has a value whose difference from one is a unit, or the coefficient is unramified and Frobenius minus one is a unit. Local restriction is injective by vanishing of the invariants over K_w. Thus at these primes unramifiedness descends too.

Now take $b \in T$. The coefficient is trivial on D_b, so local classes are additive characters. Their restrictions to wild inertia vanish since $b \neq p$. The maximal pro-p quotient of tame

inertia is procyclic. In this quotient the image of inertia over K_w has index p^{u_b}, since the image of inertia in $\mathrm{Gal}(K_w/\mathbb{Q}_b)$ has exactly that order. Hence a character is unramified over K_w precisely when its values on inertia are killed by p^{u_b}. It can take any unramified value allowed by global reciprocity. Local reciprocity identifies the tame inertia character with a character of $\mathbb{F}_b^\times$.

Restriction from $\mathbb{Q}$ to H now gives the $\widetilde{\chi}$-equivariant characters by averaging over Δ_H, whose order is prime to p. Away from T, restriction detects unramifiedness, since the corresponding inertia indices are also prime to p. At $b \in T$ the completions of H equal $\mathbb{Q}_b$. Thus finite class field theory gives the ray modulus $\mathfrak{m}$ and the indicated quotient by the multiples of the inertia images. At a prime of H over p, a stabilizer element acts on the target by a root whose difference from one is a unit. The ray class of this prime is fixed by that element. Its value must vanish, so every such ray character already satisfies local splitting at p. Real places contribute no odd-order characters. This proves the isomorphism in both directions.

At $h = 1$ the extra multiples $p^{u_b} I_b^{\mathrm{ray}}$ are automatically killed. The space $M[p]$ is finite by Theorem 22.58. The operator $\sigma - 1$ for a generator of P is nilpotent on it, since $(\sigma-1)^{|P|} = 0$ in characteristic p. Every nonzero such space has nonzero invariants. Every nonzero p-primary torsion group has a nonzero element of order p. This proves the vanishing equivalence. □

Corollary 26.25 (A unit test in the residue fields)**.** *Suppose* $\mathrm{Hom}_{\Delta_H}(\mathrm{Cl}(H), k(\chi)) = 0$. *Put* $U = \mathcal{O}_H^\times$, $V = (\mathcal{O}_H/\mathfrak{m})^\times$, *and* $e_\chi = |\Delta_H|^{-1} \sum_{\delta \in \Delta_H} \chi(\delta)^{-1} \delta \in k[\Delta_H]$. *Then*

$$\dim_k (M[p])^P = |T| - \dim_k e_\chi \,\mathrm{im}\,(U \otimes_{\mathbb{Z}} k \longrightarrow V \otimes_{\mathbb{Z}} k).$$

In particular, the residues of global units decide whether the entire P-block vanishes.

Proof. In the ray class sequence the kernel of the surjection onto $\mathrm{Cl}(H)$ is $V/\operatorname{im} U$. First take the finite p-parts, extend scalars to O, and apply $e_{\widetilde{\chi}}$, defined by the same projector with Teichmüller values. These operations preserve exactness. The projected ordinary class group has zero reduction modulo p by the character hypothesis, and is zero by finiteness. Consequently the projected ray group modulo p is the quotient of $e_\chi(V \otimes k)$ by the displayed unit image. Its dual has the required dimension by Theorem 26.24.

For each $b \in T$ one has $p \mid b - 1$. Indeed Frobenius raises a tame inertia generator to its b-th power in the abelian local quotient of $K/\mathbb{Q}$, where that generator has order p^{u_b}. The primes over b in H are permuted freely and transitively by Δ_H, and their residue fields are all canonically $\mathbb{F}_b$. Thus this part of $V \otimes k$ is one copy of the regular representation of Δ_H, contributing exactly one dimension to e_χ. Summing over b proves the formula. □

Theorem 26.26 (The cubic field of conductor 3367 in the real dyadic tower)**.** *Let K be the cyclic cubic field with the three characters at $7, 13, 37$ specified in Section 26.10. For every $J \geq 0$ and every positive even r, restriction gives*

$$\mathcal{S}_{3,r}(K) \xrightarrow{\sim} \mathcal{S}_{3,r}(KC_J) \simeq (\mathbb{Z}/3\mathbb{Z})^2.$$

On the original fields E_x this group is exactly the subgroup fixed by $\mathrm{Gal}(E_x/KC_J)$.

Proof. Split the action of $\mathrm{Gal}(C_J/\mathbb{Q})$ over an unramified coefficient extension containing its character values. The preceding descent proofs apply to KC_J directly, since the complementary factor to its cubic Sylow group is the dyadic group. For a character β of exact order $2^j > 1$ the residual character is $\bar{\beta}^{-1}$, as r is even. Its field is C_j. Its ordinary class number is prime to three by Corollary 1.1 of Fukuda and Komatsu [12].

For $v = 3, 13, 37$ one has $v_2(v^2 - 1) - 3 = 0$, and for $v = 7$ the value is one. The Frobenius order calculation of Corollary 22.60 shows that all four decomposition groups have nontrivial character image if $j \geq 2$. Theorem 22.59 kills these blocks. At $j = 1$ only 7 splits. In $H = C_1 = \mathbb{Q}(\sqrt{2})$ the two residues of $\sqrt{2}$ at 7 are $3, -3$. The unit $1 + \sqrt{2}$ has residues $4, 5$. Their discrete logarithms to base three in $\mathbb{F}_7^\times$ are $4, 5$, distinct modulo three. Conjugation exchanges the two places, so their logarithms have nonzero projection to the one-dimensional nontrivial character space. Corollary 26.25 kills this last nontrivial dyadic block as well.

The trivial dyadic block descends to K by restriction and averaging, globally and on the local kernels, since 2^J is a unit at three. The calculation over K in Theorem 26.23 gives the claimed group. The coefficient extension is faithfully flat, so restriction is already an isomorphism over $\mathbb{Z}_3$. The further extension E_x/KC_J has degree a power of two and the same restriction argument identifies its invariants. □

Thus on this whole dyadic subfield the even weights $1 \leq r < t$ contribute exactly $2\lfloor (t - 1)/2 \rfloor \log 3$ to the logarithmic sum of strict orders. The terms on which a moving quadratic acts nontrivially still enter the sum on the full period field.

26.12 Cyclic descent at every precision and the split coefficient prime

Let $E, K, P, \alpha, \theta, \chi, H, O$ and M be as in Section 22.27, and assume $\chi \neq 1$. The prime p may split completely in H. Write Q_n for the degree p^n layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, with $Q_0 = \mathbb{Q}$. Its completion at p is $Q_{p,n}$, and $Q_{p,\infty}$ denotes their union. For an integer $h \geq 1$ and a subgroup $U \leq P$, write $K_0 = K^U$ and $a = v_p([K : \mathbb{Q}])$. Put

$$n = \max\{0, h - 1 - v_p(r)\}, \qquad m = \max\{n, a\}, \qquad F = K_0 H Q_n.$$

On G_{K_0} the character $\theta \bmod p^h$ factors through $G = \mathrm{Gal}(F/K_0)$. Indeed the principal-unit part of the cyclotomic character raised to the power $-r$ is trivial modulo p^h on G_{Q_n}. This follows from $v_p((1 + p)^{rp^n} - 1) = 1 + v_p(r) + n$ for odd p. The prime-to-p part is $\widetilde{\chi}$.

Define a finite quotient $C_h(F; K)$ of the idele class group of F by the following local subgroups. All completions used together are embedded in one algebraic closure of the rational local field. The extensions in question are abelian, so the subgroups are independent of the choices and are permuted by G.

1. At $w \mid p$, take the norm subgroup from $K_v H_{v'} Q_{p,m+h}$ to F_w, where v, v' are the compatible places of K, H.

2. At $w \mid b \neq p$ where K/K_0 ramifies and $\chi(D_b) = 1$, let e_b be the ramification index of K/K_0 there. Take the group generated by the principal units and the e_b-th powers of the local units.

3. At the remaining finite places take the whole unit group. At every infinite place take the whole multiplicative group.

The local subgroups at the finitely many exceptional places contain open subgroups of the units. The quotient is consequently a quotient of a finite ray class group. The norm in the first rule is a local field norm.

Theorem 26.27 (All finite torsion over each intermediate field)**.** *With $R_h = O/p^h O$, there is an isomorphism*

$$(M[p^h])^U \simeq \mathrm{Hom}_G\left(C_h(F; K), R_h(\theta)\right).$$

In particular $U = 1$ computes the whole group killed by p^h. For $U = P$ the global field used in the computation is HQ_n.

Proof. Descent through the prime-to-p part of $E/\mathbb{Q}$ identifies M with the strict group for $A(\theta)$ over K, where $A = O[1/p]/O$, as in Theorem 22.58. The image of the nontrivial residual character on G_K is its full image, since $[K : \mathbb{Q}]$ is a power of p. Thus $A(\theta)^{G_K} = 0$. Multiplication by p^h on $A(\theta)$, with kernel identified with $R_h(\theta)$ by division by p^h, gives unique finite-coefficient lifts of $M[p^h]$. They are unramified away from p. Indeed, the inertia action there has order prime to p, so its divisible-coefficient invariants are either A or zero. The map on inertia cohomology from finite to divisible coefficients is therefore injective. An unramified class maps to zero in divisible local cohomology at such a place, since on nonzero inertia invariants Frobenius acts by a root of unity times the inverse r-th power of the residue cardinality, a scalar different from one. At p the local condition on the finite lift is that its divisible-coefficient class vanish.

The finite coefficient also has zero invariants over K. Inflation–restriction from K_0 to K identifies U-invariant global classes with global classes over K_0. Restrict these further to F. The group G is the product of Δ_H and the group of K_0Q_n/K_0, since K_0Q_n has p-power degree. The cohomology of Δ_H with coefficients $R_h(\theta)$ vanishes in every degree, including degree zero. Indeed its order is a unit and some value of $\widetilde{\chi} - 1$ is a unit. The group extension sequence then gives $H^1(G, R_h(\theta)) = H^2(G, R_h(\theta)) = 0$. Restriction identifies global classes over K_0 with G-equivariant additive characters over F.

Consider a finite place over $b \neq p$. If K/K_0 is unramified there, inertia is unchanged in this first descent. At a ramified prime for which $\chi(D_b) \neq 1$, its image remains nontrivial over both local p-extensions of $\mathbb{Q}_b$. The unramified finite subgroup is zero on both local fields, and restriction is injective by vanishing of local invariants. These assertions follow by testing inertia first and then Frobenius on its invariants, as in Theorem 26.24. In passing from K_0 to F, the inertia index is prime to p, since Q_n is unramified at b. Restriction thus detects unramifiedness in both cases.

At the exceptional tame primes H splits and F/K_0 is unramified. The finite coefficient can have nontrivial Frobenius but is trivial on inertia. Its restriction to inertia is an additive character on the procyclic p-part of tame inertia. Inertia over K maps to the subgroup of index e_b in that quotient. Thus the class is unramified over K exactly when e_b kills its inertia image. Local reciprocity over F_w gives the second rule.

Finally fix a place over p and write $L_\infty = K_v H_{v'} Q_{p,\infty}$. The coefficient $A(\theta)$ is trivial over L_∞. The group $\mathrm{Gal}(L_\infty/K_v)$ is a product of a finite group of order prime to p and an open subgroup of the cyclotomic $\mathbb{Z}_p$. Indeed it embeds with finite index in $\mathrm{Gal}(H_{v'}Q_{p,\infty}/\mathbb{Q}_p)$, which has this form by disjointness of the two factors. A generator of its procyclic factor acts on A by a scalar different from one since $r > 0$. Subtracting a coboundary can therefore kill the value of a cocycle on this generator, as multiplication by that scalar minus one is surjective on A. Density of integral powers and averaging over the finite factor give $H^1(\mathrm{Gal}(L_\infty/K_v), A(\theta)) = 0$. By inflation–restriction the local divisible class is zero over K_v exactly when it is zero on G_{L_∞}. There the action is trivial, so this is precisely the vanishing of the finite character on G_{L_∞}.

The restriction of that character to G_{F_w} must therefore factor through L_∞/F_w. To make the condition finite put $L_i = K_v H_{v'} Q_{p,i}$. The intersection of $K_v H_{v'}$ with $Q_{p,\infty}$ has degree at most p^a, since $[H_{v'} : \mathbb{Q}_p]$ is prime to p. For $i \geq m$ restriction therefore identifies $\mathrm{Gal}(L_\infty/L_i)$ with $\mathrm{Gal}(Q_{p,\infty}/Q_{p,i})$. In particular $\mathrm{Gal}(L_\infty/L_{m+h})$ is the subgroup of p^h-th powers in $\mathrm{Gal}(L_\infty/L_m)$. The latter group fixes F_w. Every character of exponent dividing p^h which factors through L_∞/F_w thus factors through L_{m+h}/F_w. The converse follows by restriction. Local reciprocity gives exactly the first norm subgroup. Global reciprocity with these local rules now gives the required isomorphism. Odd-order characters impose no further condition at real places. □

Corollary 26.28 (A ray of modulus p^2 at a split coefficient prime)**.** *Suppose p splits completely*

in H. Put

$$T = \{b \neq p : b \text{ ramifies in } K,\ \chi(D_b) = 1\}, \qquad \mathfrak{m} = p^2\mathcal{O}_H \prod_{b\in T} b\mathcal{O}_H.$$

Let K_v be the completion at p. Start with $C = \mathrm{Cl}_{\mathfrak{m}}(H)$. If $K_v \subset Q_{p,\infty}$, quotient C by the classes of the ideles equal to p at one place over p and one everywhere else, for all such places. Use C itself when $K_v \not\subset Q_{p,\infty}$. Writing C' for the resulting group, one has

$$\dim_k (M[p])^P = \dim_k \mathrm{Hom}_{\Delta_H}(C', k(\chi)).$$

In particular $M = 0$ exactly when the right side is zero.

Proof. Take $h = 1$ and $U = P$, so $F = H$ and each F_w at p is $\mathbb{Q}_p$. By local reciprocity the maximal abelian pro-p quotient over $\mathbb{Q}_p$ is the product of two copies of $\mathbb{Z}_p$, from the uniformizer and the principal units. In the cyclotomic $\mathbb{Z}_p$-extension the uniformizer acts trivially and the principal units act faithfully. In the compositum with K_v the uniformizer therefore generates a cyclic group of order $[K_v : K_v \cap Q_{p,\infty}]$ in the kernel of restriction to $Q_{p,\infty}$. To see it generates that kernel, decompose each local reciprocity element into a uniformizer power and a unit. A trivial image in the cyclotomic quotient forces the principal-unit part to be trivial. The principal-unit direction maps isomorphically to the cyclotomic quotient and has trivial intersection with this finite kernel. At exponent p, the local character is consequently arbitrary on $(1 + p\mathbb{Z}_p)/(1 + p^2\mathbb{Z}_p)$. Its value at p is free when the finite kernel is nontrivial and is zero otherwise. This gives the stated modulus and uniformizer classes. At each $b \in T$ the tame index is divisible by p, so its condition at this precision is simply the squarefree ray condition. Apply the theorem. The equivalence for the whole block follows from nilpotence of $\sigma - 1$ on $M[p]$, as in Theorem 26.24. □

Corollary 26.29 (Simultaneous tests for the moving quadratic characters)**.** *Fix an odd p dividing* $\operatorname{ord}\psi$ *and take a sufficiently distant original interval. For every α nontrivial on at least one of the two moving quadratic factors, one ray group over H decides the vanishing of M simultaneously at all positive weights in any one residue class modulo $p - 1$ of the prescribed sign. Use Corollary 26.28 when p splits completely in H, and Theorem 26.24 otherwise. The defining field H has conductor dividing* $\mathrm{lcm}(p, N_*)$*. The finite ray modulus divides $p^2 \prod_{b\neq p,\ b \text{ ramifies in } K} b\mathcal{O}_H$, where the factor p^2 also denotes its extended ideal.*

Proof. The two auxiliary primes are distinct and avoid $2p$ and the fixed conductor for all sufficiently large intervals. At the prime of a nontrivial moving factor, its quadratic inertia value survives reduction modulo odd p. The other factors and $\bar{\kappa}_p$ are unramified there, so $\chi \neq 1$. It is cut out by a character of conductor dividing the displayed least common multiple. At precision one its value depends only on α and $r \bmod (p - 1)$. The local ramification indices, the split-prime uniformizer condition and the residual field are consequently the same throughout that weight class. The two ray formulas give the conclusion, including the asserted modulus. □

Vanishing of one such character space removes its whole block from the sum in Section 6.6. If it is nonzero, the test at precision one determines the number of indecomposable summands of $M[p]$. Their lengths at higher precision still enter the required uniform bound.

26.13 Tame ramification in the moving quadratic components

Use the fields and character notation of Section 26.12, with $\chi \neq 1$. Write $S_{\mathbb{Q}}(\theta)$ for the subgroup of $H^1(\mathbb{Q}, A(\theta))$ locally zero at p and unramified away from p, with $A = O[1/p]/O$.

At a finite prime away from p its unramified local subgroup is zero, by the Frobenius calculation in Theorem 22.58. Put $s = 1+v_p(r)$, and use the set T and tame exponents u_b of Theorem 26.24, allowing either splitting behavior at p. Let w be a place of K over p, and put

$$p^\ell = [K_w : K_w \cap Q_{p,\infty}], \qquad v = \begin{cases} \min(\ell, s), & \chi(D_p) = 1, \\ 0, & \chi(D_p) \neq 1. \end{cases}$$

Theorem 26.30 (The length added by cyclic descent)**.** *Restriction gives an exact sequence at its first three terms*

$$0 \longrightarrow S_{\mathbb{Q}}(\theta) \longrightarrow M^P \longrightarrow A[p^v] \oplus \bigoplus_{b \in T} A[p^{u_b}].$$

In particular the difference of the O-lengths of M^P and $S_{\mathbb{Q}}(\theta)$ lies between zero and $v+\sum_{b\in T} u_b$. The same bounds apply to the difference of the lengths of their images under multiplication by p^j, for every $j \geq 0$.

Proof. Since $\chi \neq 1$ has prime-to-p order, $A(\theta)^{G_K} = 0$. Global inflation–restriction identifies P-invariant cohomology over K with cohomology over $\mathbb{Q}$. The local conditions for M are those over K with coefficient $A(\theta)$. Away from p, unramifiedness descends at every prime unramified in K, because inertia is unchanged. At a ramified prime with $\chi(D_b) \neq 1$, the local invariants over K_w vanish, so restriction on local H^1 is injective. The unramified local subgroup over K_w is zero. Therefore a descended strict class is locally zero at such a prime. The same injectivity holds at p if $\chi(D_p) \neq 1$.

At $b \in T$ the coefficient is unramified. Restriction of a local class to tame inertia determines it, since the unramified subgroup is zero. Wild inertia gives no p-primary character. Choose a generator of the pro-p tame inertia quotient. The condition of becoming unramified over K_w forces its value to be killed by $e_b(K/\mathbb{Q}) = p^{u_b}$. Evaluation therefore embeds the possible local images into $A[p^{u_b}]$.

If $\chi(D_p) = 1$, then over $\mathbb{Q}_p$ the full character θ is $\langle \kappa_p \rangle^{-r}$, with the brackets denoting projection to $1 + p\mathbb{Z}_p$. Its action is trivial over $Q_{p,\infty}$. Restriction to that field is injective on local cohomology. Indeed a generator of the cyclotomic $\mathbb{Z}_p$ acts on A by a scalar whose difference from one is surjective, so the first cohomology of that quotient vanishes. A class becoming zero over K_w now gives a homomorphism on $\mathrm{Gal}(K_w Q_{p,\infty}/Q_{p,\infty})$. This group is cyclic of order p^ℓ. The compositum is abelian over $\mathbb{Q}_p$, and equivariance forces the image into the fixed subgroup of $A(\theta)$ under the cyclotomic quotient. This is $A[p^s]$, by $v_p((1+p)^{-r}-1) = s$. Evaluation at a generator embeds the possible local images into $A[p^v]$.

The kernel of all these local evaluations is precisely $S_{\mathbb{Q}}(\theta)$. The assertion concerns finite groups by Proposition 11.4 and the injection just proved. Each $A[p^u]$ has O-length u. Finally multiplication by p^j induces a surjection from the original quotient of the two groups to the quotient of their images, which proves the assertion at every cutoff. □

For the fixed odd divisors p of $\operatorname{ord}\psi$, the sum of these discrepancies over all moving components and $1 \leq r < t(x)$, with their weights $\log p$, is $O_\psi([E_x : \mathbb{Q}]\, t(x))$. Indeed K depends only on p, ψ, so ℓ, the ramified primes and their indices are bounded independently of x. There are at most $[E_x : \mathbb{Q}]$ characters at each such prime. Every moving character has $\chi \neq 1$ by Corollary 26.29. This bound compares the rational strict groups with the P-fixed subgroups. The lengths of the rational groups themselves still occur in the estimate.

Theorem 26.31 (Lower bounds from the ramified primes)**.** *Let h satisfy $1 \leq h \leq s$, and let N_h count the primes $b \in T$ with $u_b \geq h$. The number of elementary divisors of M^P of length*

at least h over O is at least

$$\max\{0, N_h - 1 + \mathbf{1}_{\{\chi(D_p)=1,\ \ell \geq h\}}\}.$$

Proof. For a finite O-module B, denote the number in question by $m_h(B)$. The elementary divisor theorem identifies it both with $\dim_k(p^{h-1}B)[p]$ and with $\dim_k(p^{h-1}B/p^hB)$. Thus a submodule cannot have a larger m_h than the ambient group. Quotienting by a cyclic O-submodule decreases m_h by at most one. Indeed in the second description the kernel is the image modulo p^hB of the intersection of that cyclic submodule with $p^{h-1}B$, so it has dimension at most one.

At this precision the coefficient on the residual field is trivial. Theorem 26.24 applies if $\chi(D_p) \neq 1$. Use the ray class group there with the specified tame relations. If $\chi(D_p) = 1$, use Theorem 26.27 with $U = P$, so $F = H$. The local calculation of Corollary 26.28 works through precision h as follows. At each $w \mid p$ the principal-unit direction has quotient $(1 + p\mathbb{Z}_p)/(1 + p^{h+1}\mathbb{Z}_p)$, cyclic of order p^h. The value on the uniformizer idele is killed by p^ℓ, since its image generates the cyclic kernel of order p^ℓ in the local compositum. Thus in the split case one starts with the additional modulus $p^{h+1}\mathcal{O}_H$ and the local uniformizer relations. If $h \leq \ell$, the latter are automatically satisfied by characters into R_h.

In either computation take the p-primary part, extend scalars to O and apply $e_{\widetilde{\chi}}$. This is an exact operation since $|\Delta_H|$ is a unit. The residue-unit term in the ray class sequence has one cyclic summand on this component from each $b \in T$, as in Corollary 26.25. Its length after imposing the tame multiples is u_b, since $p^{u_b} \mid b - 1$. In the split case there is also one summand of length h from the principal units above p. Indeed those places are freely permuted by Δ_H. The order of the residue field's multiplicative group at p is prime to p.

The projected global unit group is cyclic over O. To see this, Dirichlet's unit theorem identifies the real representation on the logarithms of the units of the totally real H with the hyperplane of coordinate sum zero in the permutation representation on its embeddings. This is the regular representation less its trivial character. Its rational character therefore contains $\widetilde{\chi}$ once after extending scalars to the splitting field. The torsion in the unit group has order at most two. Hence the completed unit group on this component is a free rank-one O-module. In the ray sequence the image of the residue units, with the tame multiples imposed, is thus a submodule of the ray quotient obtained from the listed summands by one cyclic relation. More explicitly, its kernel in that residue-unit presentation is the image of the global units. This lowers m_h by at most one.

In the split case with $\ell < h$, imposing the multiples p^ℓ of all uniformizer classes costs at most one further cyclic relation on the projected ray group. The classes are an orbit indexed by the freely permuted places over p, so on this component they are generated by the projection of any one of them. This potential loss cancels the extra local principal-unit summand in the lower bound. For $h \leq \ell$ there is no loss at this step. Finally the equivariant characters into R_h are the R_h-dual of the projected group through precision h. A cyclic summand contributes to m_h of this dual exactly when its original length is at least h. The ray formulas identify that dual with $(M^P)[p^h]$, which has the same m_h as M^P. □

Corollary 26.32 (A nonzero moving component at every odd weight)**.** *Use the cubic character of conductor* 3367 *from Section 26.10, and take $p = 3$. On every sufficiently distant interval of Theorem 19.15 choose $\alpha = \eta_{-d_0}$, the quadratic character of the second auxiliary field. At every positive odd weight in the required range the P-fixed subgroup of this moving component has at least two elementary divisors. Its $\mathbb{Z}_3$-length is at least that of $S_{\mathbb{Q}}(\theta)$ and the difference is at most three. Moreover $\mathrm{Cl}(K\mathbb{Q}(\sqrt{3d_0}))$ has 3-rank at least four.*

Proof. At $p = 3$ the residual cyclotomic character is the quadratic character of $\mathbb{Q}(\sqrt{-3})$. At odd r its product with η_{-d_0} cuts out $H = \mathbb{Q}(\sqrt{3d_0})$, and 3 ramifies in H. The only primes ramified in K are $7, 13, 37$, all totally ramified of index three. They are 1 mod 3, so they split in $\mathbb{Q}(\sqrt{-3})$. The choice in Theorem 5.6 gives $d_0 \equiv -1$ at every odd prime up to a bound tending to infinity along the chosen intervals. Hence each of these three fixed primes also splits in $\mathbb{Q}(\sqrt{-d_0})$, and therefore in H. Thus $N_1 = 3$ and $v = 0$. The lower bound follows from Theorem 26.31 at $h = 1$, and the length comparison from Theorem 26.30. The character takes values in $\mathbb{Z}_3$, so its projector is already defined there. Extension to the unramified splitting ring preserves length and the number of elementary divisors.

By Theorem 22.58, the nontrivial quadratic component of the 3-class group of KH has rank at least two, by duality at precision one. On the trivial component extension of ideals embeds the 3-class group of K, since the norm of an extended class is its square, and squaring is an automorphism on a finite 3-group. This supplies two further independent directions by Lemma 26.22. The two components are disjoint since two is a unit at three. □

This example occurs on the period fields themselves, with the selected moving prime. Vanishing of all moving 3-components at all weights would be too strong. The estimate in Section 6.6 concerns their weighted lengths beyond the prescribed truncation.

26.14 All weights on a family of cyclic sextic character fields

Write ω for the order-two character of conductor three, viewed also as the Teichmüller part of the 3-adic cyclotomic character κ_3. The principal-unit part is $\langle \kappa_3 \rangle = \kappa_3/\omega$. We construct primitive characters for which the complementary-sign strict group over the entire fixed character field and every real dyadic layer can be computed at every positive weight. Their moving quadratic components on the same intervals also give lower bounds of arbitrarily large rank.

Lemma 26.33 (Realizing the cubic residue conditions)**.** *For each $m \geq 2$ there are infinitely many squarefree products of m distinct primes $b_i \equiv 13 \bmod 24$ with cubic characters $\nu_i : (\mathbb{Z}/b_i\mathbb{Z})^\times \to \mathbb{F}_3$ such that the matrix of Section 26.10 has rank $m-1$ and $\sum_i \nu_i(3) \neq 0$.*

Proof. Start with $b_1 = 13$ and discrete logarithm to base 2 modulo three. The element 2 has order 12 modulo 13 and $2^4 = 3 \bmod 13$. Thus $\nu_1(3) = 1$, and the one-row matrix is zero. Suppose $b_1, \dots, b_j$ and their characters have been chosen. Let K_i be the cubic field of ν_i. Consider the finite Galois extensions

$$M = \mathbb{Q}(\zeta_3, \sqrt[3]{3}, \sqrt[3]{b_1}, \dots, \sqrt[3]{b_j}), \qquad B = \mathbb{Q}(\zeta_3, \zeta_8) K_1 \cdots K_j,$$

using real cube roots. The group over $\mathbb{Q}(\zeta_3)$ in M embeds in a product of groups of cube roots of unity, by its multipliers on the indicated radicals. Complex conjugation inverts this group. Its commutators with conjugation exhaust the group since squaring is invertible on a group of exponent three. The maximal abelian subfield of $M/\mathbb{Q}$ is therefore $\mathbb{Q}(\zeta_3)$, so $M \cap B = \mathbb{Q}(\zeta_3)$.

The cubic factors of B are independent. A product of their characters trivial on every inertia group has exponent zero at each factor, since the i-th character alone is ramified at b_i. Their compositum has degree 3^j and is disjoint from $\mathbb{Q}(\zeta_3, \zeta_8)$, which has degree a power of two. Choose an automorphism of B fixing ζ_3, acting by fifth power on ζ_8, and having cubic coordinates $(0, \dots, 0, 1)$. It agrees on $M \cap B$ with the identity of M, so the two extend together to MB. Chebotarev's theorem for this fixed finite extension gives infinitely many unramified rational primes with this Frobenius conjugacy class. Every representative has the specified restrictions, since B is abelian and the restriction to M is the identity. See Milne, *Algebraic Number Theory*, Chapter 8 for the density theorem.

Take any such new prime b outside the previous list. We have $b \equiv 1 \bmod 3$, $b \equiv 5 \bmod 8$. Splitting in M makes $3, b_1, \dots, b_j$ cubes modulo b, so any new surjection ν_{j+1} vanishes on them. The new last column is zero in the old rows and their diagonals do not change. The new row has entry one in column j, entry minus one in column $j+1$, and its other entries are zero. Thus its addition raises the rank by one while the sum of the character values at three is unchanged. Iteration, with infinitely many choices at the last step, proves the assertion. □

Let $\varphi = \zeta_3^{\sum_i \nu_i}$ have cyclic cubic field K, and use the primitive Dirichlet character $\psi = \omega\varphi$ of conductor $3\prod_i b_i$. The local conductors are coprime. The kernel of the product is the intersection of the two kernels because their character orders are coprime. Its field is $K\mathbb{Q}(\sqrt{-3})$. For $J \geq 0$ put $L_J = K\mathbb{Q}(\sqrt{-3})C_J$. Let c be complex conjugation in this abelian field.

Theorem 26.34 (The complementary sign at every weight)**.** *For every $J \geq 0$ and every integer $r \geq 1$,*

$$\mathcal{S}_{3,r}(L_J)^{\,c=(-1)^r} \simeq (\mathbb{Z}/3\mathbb{Z})^{m-1}.$$

The real dyadic Galois group acts trivially on this part. Restriction identifies it with the same sign in the subgroup of $\mathcal{S}_{3,r}(E_x)$ fixed by $\mathrm{Gal}(E_x/L_J)$, for $J = j_x$ on the common fields of ψ.

Proof. The prime-to-three group over K is the product of the real dyadic group and $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$. After an unramified scalar extension containing its character values, the characters of the prescribed sign are $\alpha = \omega^r\beta$ with β a real dyadic character. Twisting by α^{-1} and descending to K by averaging gives coefficient character $\langle\kappa_3\rangle^{-r}\beta^{-1}$. For $\beta \neq 1$ its residual field is C_i if β has order 2^i. The primes $3, b_1, \dots, b_m$ generate the Frobenius group of each C_i. Indeed their residues are 3 or 5 mod 8, so their images in the cyclic dyadic group already generate its first quotient of order two. The class number of every C_i is prime to three by Fukuda and Komatsu [12, Corollary 1.1]. Theorem 22.59 now gives zero on this entire summand.

On the remaining summand let $\vartheta = \langle\kappa_3\rangle^{-r}$. We first show that multiplication by three kills the strict group over K with this coefficient. In the integral character comparison of Theorem 22.57 the rational scalar characters are $\xi = \vartheta\varphi^{-s}$, $s = 0, 1, 2$, over $O = \mathbb{Z}_3[\zeta_3]$. Their strong groups vanish. Here are the details for odd as well as even r. Put $\pi = \zeta_3 - 1$. Each ξ is one modulo π. In the coefficient sequence for multiplication by π, the line to quotient out of finite-character cohomology at a global or local group G is generated by $(\xi(g)-1)/\pi^{a_G} \bmod \pi$, with $a_G = \min_{g\in G} v_\pi(\xi(g)-1)$. If $\xi|_G = 1$ the connecting image is zero, by divisibility of the trivial module. For nontrivial restriction the formula follows by lifting a generator of the invariants of $O[1/3]/O$ through multiplication by π and taking its coboundary. Since $\xi(g)^2 - 1 = (\xi(g)-1)(\xi(g)+1)$ and $\xi(g)+1 \equiv 2 \bmod \pi$, the minimum and the line are the same for ξ^2. The residual character is trivial in both cases. Thus the same finite characters pass the local tests and the same line is divided out globally. This includes the inertia tests away from the prescribed primes. It identifies the π-torsion of the two strong groups. Now $\xi^2 = \kappa_3^{-2r}\varphi^{-2s}$, whose strong group is zero by Lemma 26.21 at the positive even weight $2r$. A nonzero π-primary group has nonzero π-torsion, so the assertion follows for ξ. The forward and reverse integral character maps in Theorem 22.57 compose to multiplication by $[K:\mathbb{Q}] = 3$. Factoring this composite through the zero scalar groups proves the exponent bound, also over $\mathbb{Z}_3$ by faithful flatness.

To compute the resulting group take coefficients over $\mathbb{Z}_3$. Its residual character is trivial. The prime w above three is unique and unramified of degree three by the condition $\sum \nu_i(3) \neq 0$. The local and global images of the principal-unit part of the cyclotomic character are both $1 + 3\mathbb{Z}_3$, since the local cyclotomic tower is totally ramified and the local extension at w is unramified.

The global connecting line therefore restricts isomorphically to the line at w. Subtracting its unique required multiple gives each strict class a unique finite character zero at w. At other places the coefficient is unramified, so the finite character is unramified on inertia. Conversely an unramified finite character zero at w satisfies these conditions in the divisible coefficient. By class field theory this group is the dual modulo three of $\mathrm{Cl}(K)/\langle [w] \rangle$. The ideal $w = (3)$ is principal. Lemma 26.22 gives its dimension $m - 1$. This proves the formula and the dyadic action assertion. Finally the extension from L_J to the full field has degree a power of two. Restriction and averaging preserve the global classes and detect the local kernels, giving the last assertion. □

Corollary 26.35 (A moving quadratic component at the same weights)**.** *For these characters, take $\alpha = \omega^{r-1}\eta_{-d_0}$ on E_x on the intervals of Theorem 19.15. For every sufficiently distant interval and all $1 \le r < t(x)$, the subgroup fixed by the cubic Sylow group P in this component has at least $m-1$ elementary divisors. Its length exceeds the rational strict length by an integer in $[0, m]$. The 3-class rank of $K\mathbb{Q}(\sqrt{3d_0})$ is at least $2(m-1)$.*

Proof. This α has the required sign. At every weight the residual character of $\kappa_3^{-r}\alpha^{-1}$ equals $\omega\eta_{-d_0}$, cutting out $H = \mathbb{Q}(\sqrt{3d_0})$. It is ramified at three. The b_i are all 1 mod 3; they split in $\mathbb{Q}(\sqrt{-3})$ and also in $\mathbb{Q}(\sqrt{-d_0})$ since $d_0 \equiv -1 \bmod b_i$ on the selected intervals by Theorem 5.6. Thus all m primes split in H and have ramification index three in K. Apply Theorems 26.31 and 26.30 with $h = 1$ and zero loss at three. Theorem 22.58 at precision one puts at least $m-1$ directions on the nontrivial quadratic part of the class group of KH by duality. Extension of ideals from K injects its 3-part into the trivial quadratic part since norm after extension is squaring. Lemma 26.22 supplies $m - 1$ further directions there. □

Thus the contribution from the complementary sign fixed by the moving factors in the theorem is exactly $(t-1)(m-1)\log 3$ for an integer cutoff $t \ge 1$. Its image under multiplication by three is zero. The length of the moving component in the corollary still depends on the rational strict group and the part outside P-invariants.

27 Cyclotomic indices at finite primes

27.1 Cyclotomic indices and strict orders

Let ℓ be an odd prime, α a primitive Dirichlet character of conductor f, and $r \ge 1$. Assume that $\ell \nmid f\varphi(f)$ and $\alpha(-1) = (-1)^r$. Take $O = \mathbb{Z}_\ell[\alpha]$ in a fixed algebraic closure, $J = \mathrm{Frac}(O)$, and $k = r + 1$. This ring is an unramified discrete valuation ring. Write

$$T = O(\alpha\kappa_\ell^k), \qquad A = (J/O)(\alpha^{-1}\kappa_\ell^{-r}).$$

Let $S(A)$ be the strict group over $\mathbb{Q}$ of Theorem 24.1. Put $U = \operatorname{Spec}\mathbb{Z}[1/\ell]$. For $H^i(U, T)$ use the direct image from the generic point, so that the stalk at a finite prime of U consists of the inertia invariants. Cohomology of the integral lattice is understood by passage to the inverse limit of finite coefficients.

Choose compatible primitive roots ζ_m and a generator t_α of $O(\alpha)$. For $h \ge 1$ take the Kummer class of $1 - \zeta_{f\ell^h}$ over $\mathbb{Q}(\zeta_{f\ell^h})$ at exponent ℓ^h, and tensor it with $\zeta_{\ell^h}^{\otimes r} \otimes t_\alpha$. The result has coefficients in $T/\ell^h T$. Corestrict it to $\mathbb{Q}$. These are the reductions of the Soulé–Deligne class $c_{\alpha,k} \in H^1(U, T)$. Indeed the norm of the unit from level $h+1$ to h is $1 - \zeta_{f\ell^h}$, by multiplying $1 - X$ over the roots of $X^\ell - \zeta_{f\ell^h}$. The tensor factors at precision ℓ^h are already defined over level h. This gives compatibility by the projection formula. The unit is integral outside ℓ, including when $f = 1$. This is the construction in Huber and Kings, Definitions 3.1.1–3.1.3.

Theorem 27.1 (Length of the strict group in a cyclotomic lattice)**.** *The module $H^1(U,T)$ is free of rank one over O. Write $c_{\alpha,k}=au$ for an O-basis u. Then $a\neq 0$ and*

$$v_\ell(a)=\operatorname{length}_O S(A)+\operatorname{length}_O H^0(\mathbb{Q}_\ell,A)-\operatorname{length}_O H^0(\mathbb{Q},A).$$

In particular $v_\ell(a)$ bounds the full length from above. For $\ell>2$ and $0<r<\ell-1$, the two invariant groups vanish and equality holds with $\operatorname{length}_O S(A)$.

Proof. Let $D=\mathbb{Q}(\zeta_f)$ and $G=\mathrm{Gal}(D/\mathbb{Q})$. Over D the coefficient T is the ordinary Tate lattice with a chosen basis for its finite character. Cohomology on U is the G-invariant part of the cohomology of $\mathcal{O}_D[1/\ell]$ with this character included in the action. In fact under the finite map of spectra the pushforward at a geometric point has one summand for each point above it and has no higher direct images, by proper base change at finite coefficients. The invariants of that permutation sheaf tensored with T have generic fiber T and stalk T^{I_v} at v. Averaging by $|G|^{-1}$ is integral and exact. Taking inverse limits gives the assertion for T. The same argument identifies the finite-character descent globally and locally in the duality sequence of Theorem 25.1. More explicitly, dualizing sends the isotypic factor to its inverse character, and summing over the places over ℓ gives the invariants for one decomposition group. The trace pairing identifies the O-dual into J/O with the usual Pontryagin dual here. Thus $H^2(U,T)$ is finite and its length is the right side of the asserted formula. The finiteness also follows from its inclusion as a summand of the ℓ-adic even K-group. All statements apply to $D=\mathbb{Q}$ at an odd prime.

Complex conjugation acts on T by -1. Consequently $H^0(U,T/\ell T)=0$, and the multiplication sequence shows that $H^1(U,T)$ has no ℓ-torsion. Its rank is one. Indeed the global Euler characteristic over $\mathbb{Q}$ is minus the dimension of the odd subspace, and both $H^0(U,T)$ and $H^2(U,T)$ have rank zero. Equivalently, one may calculate on the open set also removing f. At each prime removed there the primitive character is nontrivial on inertia of order prime to ℓ in its image. The inertia invariants of $T\otimes J$ and its (-1)-twist are zero, so the unramified-extension stalk and the degree-one inertia term make no rational contribution. The finite generation in the global Euler characteristic theorem now gives the stated free rank.

We use the integral main conjecture for Dirichlet characters in the form proved by Huber and Kings. For ℓ odd and $\alpha(-1)=(-1)^{k-1}$, their cyclotomic class generates the inverse determinant of the global Iwasawa cohomology complex. Specialization at the trivial character of the cyclotomic $\mathbb{Z}_\ell$-extension gives the inverse determinant of $R\Gamma(U,T)$. Huber and Kings, Theorem 4.4.1 and the specialization argument of Theorem 5.1.1.

Here is why specialization gives the actual class in degree one. Derived specialization is the triangle for multiplication by $\gamma-1$ on the inverse-limit complex, where γ generates the cyclotomic tower. This follows by Shapiro’s lemma from the sequence for multiplication by $\gamma-1$ on the completed group ring. The cokernel in degree two is the finite $H^2(U,T)$, since degree three vanishes at odd ℓ. After localizing the Iwasawa algebra at $(\gamma-1)$, Nakayama’s lemma therefore kills degree two. Degree one has no $(\gamma-1)$-torsion there, by the same triangle and the vanishing in degree zero downstairs. The determinant consequently specializes on the rational cohomology line by taking the base layer of the norm-compatible classes. In Definition 4.1.7 of the cited paper this layer is a corestriction from $\mathbb{Q}(\zeta_\ell)$. At precision ℓ^h, taking the norm from $f\ell^{h+1}$ to $f\ell^h$ first gives exactly the class defined above. The alternative normalization removing the Euler factor at ℓ changes the lattice generator by a unit since $k>1$.

Over a discrete valuation ring the inverse determinant of this complex, inside $H^1(U,T)\otimes J$, is $\ell^{\operatorname{length}_O H^2(U,T)}H^1(U,T)$. To see the sign, a cyclic summand O/ℓ^j in degree two is represented by $O\xrightarrow{\ell^j}O$ in degrees one and two. The inverse determinant basis maps to ℓ^j. Multiplying

over the elementary divisors proves the formula and shows $a \neq 0$. Global invariants inject into local ones. If $0 < r < \ell - 1$, tame cyclotomic inertia at ℓ contains a scalar whose $(-r)$-th power differs from one modulo ℓ, and α is unramified there. This kills both invariant groups. □

27.2 The distribution of the cyclotomic valuations

Fix the interval, list of triples and precisions of Theorem 21.9. In particular the original period fields, their splitting conditions and the power-residue conditions are included in the field K of that theorem. Write $j = (\ell, r, [\alpha])$ for a triple, with one representative of its residual Frobenius orbit, and put $\ell_j = \ell$. Write $h_j = h_\ell$, $b_j = [\mathbb{F}_\ell(\bar{\alpha}) : \mathbb{F}_\ell]$ and $d_j = \operatorname{length}_{O_j} S(A_j)$, where $O_j = \mathbb{Z}_\ell[\alpha]$. At a prime s split in K set

$$W_j(s) = w_{h_j}(D_{s,h_j}(\alpha, r)), \qquad m_j = \min(d_j, h_j).$$

The moment, its valuation and the convention $w_h(0) = h$ are those of Proposition 9.5. Probability below means relative natural density among the rational primes split in K.

Theorem 27.2 (Joint distribution at every precision)**.** *For any integers $0 \le k_j \le h_j$,*

$$\Pr(W_j(s) \ge k_j \text{ for all } j) = \prod_j \ell_j^{-b_j \max(0, k_j - m_j)}.$$

Thus the valuations from the different triples are independent, including different twists at the same coefficient prime. The whole law of the excess $W_j - m_j$ is that of the valuation of a uniform element modulo $\ell^{h_j - m_j}$, with truncation at $h_j - m_j$.

Proof. Choose one integral basis class u_j as in Theorem 27.1 for each triple. The character $\alpha\kappa_\ell^{r+1}$ is trivial on G_K at precision ℓ^{h_j}. A cocycle for u_j, restricted to G_K and reduced at that precision, is consequently an additive homomorphism into O_j/ℓ^{h_j}. Its value on this subgroup is independent of the cocycle representative.

The joint map of these homomorphisms is onto. To see this, fix ℓ and write $M = \prod_{j:\,\ell_j = \ell} O_j/\ell^{h_j}$, where the product is over this prime. The argument of Theorem 21.9 shows that the image modulo ℓ is $M/\ell M$. It applies to this K, including its prescribed radicals. In detail, a primitive residual class stays nonzero over K. Its coefficient module is simple over $\mathbb{F}_\ell$, and its conjugates span that simple module. Distinct listed twists have different characters on inertia at ℓ. Within one twist the simple modules are distinct precisely after the Frobenius conjugates have been identified. The idempotents for these residual characters therefore separate the factors. If I is the image at the stated precisions, this proves $M = I + \ell M$. The abelian group M/I is killed by a power of ℓ and equals $\ell(M/I)$, so it is zero. The joint image across all ℓ is the product too. In a subgroup of a finite abelian product of primary groups one isolates each primary coordinate by integer multiplication, using the Chinese remainder theorem.

The kernel of the joint map on G_K is open and normal in $G_\mathbb{Q}$. Indeed conjugation by a global element acts on each evaluation by the character of its coefficient module. The term from changing a cocycle representative vanishes on G_K. The kernel thus defines a finite Galois field over $\mathbb{Q}$. Its group over K is the full additive product just calculated. Every condition on the valuations alone defines a conjugacy-stable subset. Chebotarev's theorem therefore gives its fraction in this product as its relative density among split primes. This argument is only applied to valuation conditions, so choices of generators of residue fields have no bearing on the density.

At the large primes in the list the invariant correction in Theorem 27.1 is zero. The cyclotomic class is therefore ℓ^{d_j} times a unit times u_j. Proposition 9.5 identifies its local valuation

with $W_j(s)$. For a uniform element of O_j/ℓ^{h_j} the condition of belonging to $\ell^a O_j/\ell^{h_j}$ has probability $\ell^{-b_j a}$ for $0 \le a \le h_j$. Multiplication by the class coordinate and truncation give the claimed formula for each factor. Multiplication of these fractions gives the joint law. □

27.3 The cyclotomic index at an arbitrary odd prime

Let p be odd, $f \mid N$, and α a primitive Dirichlet character of conductor f, viewed p-adically. Take $r \ge 1$ with $\alpha(-1) = (-1)^r$, and set $k = r + 1$. Let $O = \mathbb{Z}_p[\alpha]$, $J = \mathrm{Frac}(O)$, and fix a uniformizer π. This is the integer ring of a local cyclotomic field. Write $b = [O/\pi : \mathbb{F}_p]$, $e = v_\pi(p)$, $T = O(\alpha\kappa_p^k)$, and $U_N = \operatorname{Spec}\mathbb{Z}[1/(Np)]$.

Theorem 27.3 (The index on the common open set)**.** *The module $H^1(U_N, T)$ is free of rank one. The Soulé–Deligne class $c = c_{\alpha,k}$ restricts there to a nonzero multiple of a basis. If $d = d_{p,r,\alpha}(N)$ is the π-valuation of its coordinate, then*

$$\operatorname{length}_O H^2(U_N, T) = d + \sum_{\substack{q \mid N,\ q \text{ prime} \\ q \ne p,\ q \nmid f}} v_\pi(1 - \alpha(q) q^r).$$

The formula includes p dividing the conductor, the order of α, or the degree of its full cyclotomic field.

Proof. On U_N the lattice is unramified and its cohomology is restricted-ramification Galois cohomology. In rational degree two it is a summand after passing to the field cut out by α. Over that field the coefficient is a Tate twist, whose rational degree two vanishes by the even K-group comparison of Theorem 25.1. At odd p this comparison applies also over real fields. Inverting the additional primes preserves rational vanishing, since the positive K-groups of their finite residue fields are finite. Global finite generation now gives finite integral degree two. Degree zero vanishes even modulo π, since complex conjugation acts by -1. The multiplication sequence for π gives torsion freeness in degree one. The rational Euler characteristic over $\mathbb{Q}$ is minus the dimension of the odd subspace. It gives rank one.

Put $U = \operatorname{Spec}\mathbb{Z}[1/p]$ and extend T to U by the ordinary generic-point direct image. We use the integral main conjecture of Huber and Kings in its full Dirichlet-character form. For this parity and $p \ne 2$, the cyclotomic class generates the inverse determinant of the global cyclotomic Iwasawa complex. Their theorem includes the primes dividing $\varphi(f)$. Their coefficient field can be enlarged beyond J, since an equality of lattices over a discrete valuation ring descends under finite faithfully flat extension. The defining class at precision p^h is the corestriction from $\mathbb{Q}(\zeta_{fp^h})$ of the Kummer class of $1 - \zeta_{fp^h}$ tensored with $\zeta_{p^h}^{\otimes r}$ and the character basis. This description also holds when $p \mid f$, by transitivity of corestriction. Removing a redundant p-level uses the norm of $1 - \zeta_{fp^{h+1}}$ to $1 - \zeta_{fp^h}$. Huber and Kings, Definitions 3.1.1–3.1.3, 4.1.7 and Theorem 4.4.1.

Here specialization gives the actual class on the rational cohomology line. Indeed the tower coefficient modulo $\gamma - 1$ is the base coefficient for a topological generator γ. Shapiro's lemma and the multiplication triangle give derived specialization to $R\Gamma(U, T)$. The tower is unramified away from p, so the inertia invariants in the direct image on U commute with adjoining this free tower coefficient. Rationally the specialized complex is concentrated in degree one. To see this last point one may open the primes $q \mid N$ as below. Their rational local complexes are acyclic, since $r > 0$. At the height-one prime $(\gamma - 1)$, cancel unit entries in a bounded free representative of the Iwasawa complex. The remaining differentials reduce to zero. Its rational special fiber has dimension one in degree one, leaving a single free generator in that degree. The determinant generator therefore specializes on the rational line by taking the base layer of the norm-compatible classes. This is c by the corestriction formula. In particular $c \ne 0$.

We compute the effect of removing $q \mid N$, $q \neq p$. The cone from the direct-image complex on U to the complex on U_N has at q the term $R\Gamma(\mathbb{F}_q, H^1(I_q, T))[-1]$. This follows from the stalks of the derived direct image and the p-cohomological dimension one of inertia I_q. It holds first for the finite coefficient systems and then in their inverse limit, by stabilization of the finite images. When $q \nmid f$, the inertia term is $T(-1)$. Hence the cone has zero degree one and a finite degree two of length $v_\pi(1 - \alpha(q)q^r)$. When $q \mid f$, the inertia term is finite. Indeed first take invariants of wild inertia and of the prime-to-p part of tame inertia. These are exact operations. If their invariants survive, one computes degree one by the cokernel of $\tau - 1$ on the lattice for a generator of the tame pro-p quotient. A nontrivial ramified character remaining here has $\alpha(\tau) \neq 1$, giving a finite cokernel. On this finite module the kernel and cokernel of Frobenius minus one have the same order. Thus its cone has inverse determinant of valuation zero.

Under the rational identification of the two degree-one lines, the inverse determinant for the open complex is consequently generated by c times the product of the unramified local factors, up to a unit. For U_N the same inverse determinant is $\pi^{\operatorname{length}_O H^2(U_N,T)} H^1(U_N, T)$. Indeed restricted Galois cohomology over $\mathbb{Q}$ has degree at most two at odd p, and a cyclic group in degree two contributes its elementary divisor to that lattice. Comparing valuations proves the formula. □

27.4 Cyclotomic classes that reduce to rational Kummer classes

Use the rank-one group and its cyclotomic class c in Theorem 27.3. For each odd p, write O for the character integer ring, π for its uniformizer, $e = v_\pi(p)$, $b = [O/\pi : \mathbb{F}_p]$ and $d = d_{p,r,\alpha}(N)$. Set

$$u = \min_{g \in G_{\mathbb{Q}}} v_\pi\big(\alpha(g)\kappa_p(g)^r - 1\big).$$

The value is finite since $r \geq 1$ and the cyclotomic character has infinite image on the kernel of the finite character. Here the conductor f of α divides N.

Theorem 27.4 (The rational Kummer contributions at all odd primes)**.** *If $u \geq 1$ and f is a power of p, including $f = 1$, then $d = 0$. If $u \geq 1$ and some prime other than p divides f, then $d \geq u$. On a field E_x of Theorem 19.15 the total contribution of these known initial u layers in the second case, with their weights $b \log p$, is at most*

$$[E_x : \mathbb{Q}]\, t(x) \sum_{\substack{p \mid \operatorname{ord}(\psi) \\ p \text{ odd}}} \frac{\log p}{p - 1}.$$

In particular the trivial-character index vanishes for every odd p and every positive multiple r of $p - 1$.

Proof. For $1 \leq v \leq u$ put $h = \lceil v/e \rceil$. The line with character $\alpha\kappa_p^r$ is trivial modulo π^v. Choose its fixed basis given by the tensor of the character basis and the chosen Tate basis. The defining formula for c at precision p^h is the corestriction of the Kummer class of $1 - \zeta_{fp^h}$ tensored with that basis. Reduction to O/π^v makes the basis a constant in the corestriction. Thus the reduced global class is the Kummer class of

$$N_{\mathbb{Q}(\zeta_{fp^h})/\mathbb{Q}}(1 - \zeta_{fp^h}) = \Phi_{fp^h}(1)$$

with the indicated coefficient extension. Indeed corestriction of the Kummer connecting homomorphism is the connecting homomorphism of the field norm. This follows by multiplying the conjugates of a chosen p^h-th root, whose p^h-th power is that norm. The finite-level class and twist convention are those in Theorem 27.3. A. Huber and G. Kings, Sections 3.1 and 4.1.

For $n > 1$ one has $\prod_{j\mid n,\ j>1} \Phi_j(1) = n$ by dividing $X^n - 1$ by $X - 1$ before evaluating at one. The prime-power factors each have value their underlying prime by their geometric sums. Induction on n gives value one at every n divisible by two distinct primes. In the prime-power case take $v = 1$. The Kummer class of p over $\mathbb{Q}$ modulo p is nonzero by its valuation at p, and extension to the residue field O/π is injective on this class by a choice of an $\mathbb{F}_p$-linear retraction. In the other case the Kummer class of one vanishes for all $v \le u$. Inflation in degree one from the restricted Galois group to the absolute group is injective for these coefficients. The multiplication sequence of $O(\alpha\kappa_p^{r+1})$ shows that the kernel of reduction modulo π^v on H^1 is exactly $\pi^v H^1$. Since H^1 is free on one generator, the two assertions about d follow.

In the second case take a prime $q \mid f$, $q \neq p$. The cyclotomic character at p is trivial on q-inertia. The image of α there is nontrivial by primitivity. If $u \ge 1$, it reduces to one and hence has p-power order. Its image contains a primitive p-th root ζ. Then $u \le v_\pi(\zeta - 1) = e/(p-1)$, by the factorization of $\Phi_p(1) = p$ and the equality of the valuations of the factors. In particular $p \mid [E_x : \mathbb{Q}]$. The degree over the field of the fixed character ψ is a power of two on these intervals, so $p \mid \operatorname{ord}(\psi)$. For each p, r the sum of be over the character orbits is at most $[E_x : \mathbb{Q}]$ by character decomposition in characteristic zero. This proves the uniform estimate. For $\alpha = 1$ and $p - 1 \mid r$, the residual cyclotomic character to the power r is trivial, giving the last assertion. □

27.5 A vanishing result for fields ramified at one prime

Theorem 27.5 (The strict group with an inert coefficient prime)**.** *Let p be odd and $a \ge 1$. Let B be the degree-p^a subfield of $\mathbb{Q}(\zeta_q)$ for a prime $q \neq p$, and assume that p is inert in B. For every positive multiple r of $p - 1$,*

$$\mathcal{S}_{p,r}(B) = 0.$$

For each p, a there are infinitely many such q. On the common intervals for any character cutting out B, the $\mathrm{Gal}(E_x/B)$-invariant strict group has the same vanishing. For $p = 3$ its complementary-sign part vanishes at every twist.

Proof. We first show that p does not divide the class number of B. Let H be its Hilbert p-class field. This is Galois over $\mathbb{Q}$, since its defining property is preserved by every automorphism of B. Write $G = \mathrm{Gal}(H/\mathbb{Q})$, a finite p-group. Only q can ramify. Its inertia group I maps isomorphically onto $\mathrm{Gal}(B/\mathbb{Q})$, by total ramification in $B/\mathbb{Q}$ and absence of ramification in H/B. If I were proper in G, it would be contained in a maximal subgroup. Every maximal subgroup of a finite p-group is normal of index p. The corresponding cyclic degree-p field would be unramified at q, because that subgroup contains all conjugates of I. It would be unramified at every other finite prime, and also at infinity since p is odd. The class number of $\mathbb{Q}$ excludes this by class field theory. Thus $I = G$, giving $H = B$.

Put $A = (\mathbb{Q}_p/\mathbb{Z}_p)(-r)$. The cyclotomic image over B and over its unique completion B_w at p is $\mathbb{Z}_p^\times$. Indeed $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ is totally ramified, while $B_w/\mathbb{Q}_p$ is unramified. The global image contains this local image. Thus $A^{G_B} = A^{G_{B_w}}$ inside A. For $G = G_{B,S_p}$ the exact sequence for multiplication by p gives

$$0 \longrightarrow A^G/pA^G \longrightarrow H^1(G, A[p]) \longrightarrow H^1(G, A)[p] \longrightarrow 0.$$

The local row is the same, and restriction identifies the two left terms because there is just one prime above p. It follows that the localization kernels in the middle and on the right are isomorphic. Since $p-1 \mid r$, $A[p]$ is the constant module $\mathbb{F}_p$. The middle kernel therefore consists of homomorphisms from the ideal class group of B to $\mathbb{F}_p$ that kill the class of w, by the Hilbert

class field theorem. It is zero. Any nonzero p-primary torsion group has an element of order p, which proves the claimed vanishing.

For existence let $C = \mathbb{Q}(\mu_{p^a})$. The real degree-$p$ field $\mathbb{Q}(p^{1/p})$ is not normal, since it omits the nonreal roots of $X^p - p$. It cannot be a subfield of the abelian field C. Since $\mu_p \subset C$, Kummer theory gives a cyclic degree-p extension $C(p^{1/p})/C$, Galois over $\mathbb{Q}$ as a splitting field after adjoining C. Chebotarev applied to the conjugacy class of a nonidentity element over C yields infinitely many unramified rational primes q split in C for which p is a non-p-th power in $\mathbb{F}_q^\times$. In particular $p^a \mid q-1$. The image of p generates the quotient of order p^a of the cyclic group $\mathbb{F}_q^\times$, since its exponent on a generator is prime to p. This gives the asserted inertness.

In Theorem 19.15 the relative degree $[E_x : B]$ is a power of two for these characters. Restriction identifies the strict group with the invariant part upstairs. Indeed averaging gives the isomorphism in global cohomology, and restriction is injective in local cohomology and on inertia by the prime-to-p degrees. This preserves the local conditions in both directions. For $p = 3$ the even twists are the multiples of $p-1$. The field B is real, so complex conjugation acts trivially on its group, and the complementary sign is negative for each odd twist. □

27.6 Two Frobenius evaluations at conductor 1799

Use $\chi = (\,\cdot\,/257)$, the cubic character λ mod 7 with $\lambda(3) = \zeta_3$, and $U = \operatorname{Spec}\mathbb{Z}[1/(3\cdot 7\cdot 257)]$ as in Theorem 26.18. For r positive and even, let L_0, L_1 be the two lines of Theorem 19.25 for $\chi, \chi\lambda$. Their common residual coefficient is $\bar{T} = \mathbb{F}_3(\chi\omega)$, where $\omega = \kappa_3$ mod 3.

Proposition 27.6 (The two residue lines in each even weight)**.** *One has $L_0 = L_1$ exactly when $6 \mid r$. In each of the other two even residue classes the lines span $H^1(U, \bar{T})$.*

Proof. Write c_0, c_1 for the two cyclotomic classes and $\pi = \zeta_3 - 1$. Their coordinate valuations are both one by Theorem 26.18. Thus the reductions of $c_0/3$ and c_1/π generate L_0, L_1. The cohomology group $H^1(U, \bar{T})$ has dimension two. Indeed the multiplication-by-three sequence for the first lattice gives one dimension from its free rank-one group in degree one and one from its degree-two group of order three. This calculation applies to a single residual module for all even r, since $\omega^r = 1$.

Use the two rational primes and generators (s, g) in the table. Both $s-1$ are multiples of $9\cdot 7\cdot 257$. At each prime choose the place in the common cyclotomic field where a compatible primitive root ζ_n reduces to $g^{(s-1)/n}$ for each $n \mid 9\cdot 7\cdot 257$. These assignments come from the single root of the largest order. Evaluating a residual cocycle at the corresponding arithmetic Frobenius gives a linear form, since that Frobenius acts trivially on $\bar{T}$ and coboundaries give zero. Choose the tensor bases in all even weights by identifying $\zeta_3^{\otimes(r+1)}$ with the fixed residual basis and taking the finite character basis for λ to reduce to one. These local choices define the same pair of linear forms when comparing the two classes and all three weights.

For the first class compute the six entries B_i of Theorem 27.8, in the order $1, 2, 4, 5, 7, 8$. For the second compute the three C_j of Theorem 26.18. Use the indicated roots w_0, w_1 of orders $2313, 5397$ for the respective computations.

s	g	w_0	w_1	(B_i) mod 9	(C_j) mod 3
129529	37	63673	59753	$(7,6,2,2,6,7)$	$(2,1,0)$
161911	3	131000	88463	$(5,6,4,4,6,5)$	$(2,1,0)$

Trial division to 359 and 402, respectively, tests primality. The residues $g^{(s-1)/d}$ at the distinct prime divisors d of $s-1$, taken in increasing order, are $(129528, 120445, 60611, 35657)$ for $d = 2, 3, 7, 257$ and $(161910, 47683, 63009, 55156, 24972)$ for $d = 2, 3, 5, 7, 257$. For an alternative

direct verification of the two last columns, list g^j mod s for $0 \le j < s-1$, labeling each residue by j. For each defining sum multiply $1 - w^a$ over the indices belonging to its specified residue class and having $\chi(a) = 1$, then divide by the same product for $\chi(a) = -1$. Read the label of the result modulo nine or three, respectively. This gives the entries by additivity of the logarithm.

In the chosen bases the first Frobenius coordinate before division is $\sum_i B_i i^r$ mod 9. For the second it is $\sum_j C_j(1 + j\pi)$ mod π^2. To check the normalizations, restriction of the corestriction is a sum over a prime to the conductor times the coefficient modulus. Conjugation sends $1 - \zeta_n$ to $1 - \zeta_n^a$ and acts on the extra tensor factor by $\chi(a)a^r$, with an additional $\lambda(a)$ for the second class. The Kummer cocycle of a residue z at Frobenius has value $z^{(s-1)/p^h}$ for modulus p^h. Its coordinate in the reduction of ζ_{p^h} is exactly $\operatorname{ind}_g z$ mod p^h. This gives both formulas with compatible bases. The two Frobenius elements already act trivially at the precision of each numerator, so that division gives the evaluations of the integral quotients in residual cohomology.

In the order of the table the coordinate vector for c_1/π is $(1, 1)$ at every even twist. For $c_0/3$ the vectors at $r \equiv 0, 2, 4$ mod 6 are, respectively, $(1, 1), (0, 2), (2, 0)$ in $\mathbb{F}_3^2$. In residue class two the two vectors are independent, so the evaluation map from the common two-dimensional cohomology group is injective. Equality and independence of the lines in the other residue classes can therefore be read from the same two coordinates, which proves the result. □

27.7 Class groups and strict classes throughout one cyclotomic extension

Put $F = \mathbb{Q}(\sqrt{257}, \zeta_7 + \zeta_7^{-1})$, $Q_m = \mathbb{Q}(\zeta_{3^{m+1}})^+$, $F_m = FQ_m$ for $m \ge 0$, and $L = \bigcup_{m \ge 0} F_m$. Thus $Q_0 = \mathbb{Q}$. The prime 3 is inert of degree six in F. Its Frobenius has order two on $\mathbb{Q}(\sqrt{257})$ and order three on $\mathbb{Q}(\zeta_7)^+$. The extension $Q_m/\mathbb{Q}$ is totally ramified at 3, so $F \cap Q_m = \mathbb{Q}$ and F_m has just one prime over 3. Let $\Gamma = \operatorname{Gal}(L/F)$ and take γ with image 4 in $1 + 3\mathbb{Z}_3$. Here the projection of the cyclotomic character to principal units identifies Γ with $1 + 3\mathbb{Z}_3$. Indeed $v_3(4^{3^i} - 1) = 1 + i$ by induction and binomial expansion.

Let C_m be the 3-part of the ideal class group of $\mathcal{O}_{F_m}[1/3]$, and $X = \varprojlim C_m$ under the ideal norms. The group $\operatorname{Gal}(L/\mathbb{Q})$ acts on X. For δ in this group, write $u(\delta) \in 1 + 3\mathbb{Z}_3$ for its principal cyclotomic character.

Theorem 27.7 (Untwisted and twisted quotients of the same class group limit)**.** *For every m, $C_m = \operatorname{Cl}(F_m)\{3\}$ and $C_m \simeq X/(\gamma^{3^m} - 1)X$. Let $D \subset L$ be a number field such that L/D is unramified away from 3 and $\operatorname{Gal}(L/D) \simeq \mathbb{Z}_3$ has generator δ with $u(\delta) \ne 1$. For $r \ge 1$ put $A_r^{\mathrm{pr}} = (\mathbb{Q}_3/\mathbb{Z}_3)(\langle \kappa_3 \rangle^{-r})$, where the brackets remove the sign of the 3-adic unit. With the same strict local conditions one has*

$$S(D, A_r^{\mathrm{pr}})^\vee \;\simeq\; X/(\delta - u(\delta)^{-r})X.$$

At even r this is the dual of $\mathcal{S}_{3,r}(D)$. The identification uses a fixed basis of the coefficient on G_L.

Proof. The prime over 3 in Q_m is generated by $(1 - \zeta_{3^{m+1}})(1 - \zeta_{3^{m+1}}^{-1})$. Its norm to $\mathbb{Q}$ is three, by the cyclotomic polynomial at one. Over Q_m the extension F_m is unramified at this prime with a single prime above it, so the same element generates that prime in F_m. Inverting it preserves the class group.

Let H_j/F_j be the class field of C_j, so that the prime over 3 splits completely there. For $j \ge m$, $H_m \cap F_j = F_m$, by total ramification in F_j/F_m. Base change gives $H_m F_j \subset H_j$. Under reciprocity restriction of automorphisms gives the norm $C_j \to C_m$, which is therefore

surjective. In the extension H_j/F_m the decomposition group at the single prime over 3 maps isomorphically onto $\mathrm{Gal}(F_j/F_m)$. Thus $\mathrm{Gal}(H_j/F_m)$ is a semidirect product of C_j with this cyclic decomposition group. Its largest abelian quotient in which the prime splits is obtained by killing a generator of the latter group and its conjugates. It is $C_j/(\gamma^{3^m}-1)C_j$. The corresponding field is unramified everywhere, split at 3, and contains H_m, so is exactly H_m. This proves the finite quotient formula. Passing to X preserves the kernel description. Indeed all projections from X are surjective. Given compatible elements in the kernels, the conditions on a preimage under $\gamma^{3^m}-1$ at finitely many levels can be met at their largest level. Compactness supplies a preimage at all levels.

For the twisted formula put $A = A_r^{\mathrm{pr}}$. Its action factors through the principal-unit cyclotomic quotient and is therefore trivial on G_L. At even r the sign of a 3-adic unit disappears on raising it to the r-th power. The procyclic quotient $\mathrm{Gal}(L/D)$ has zero degree two on A and degree one $A/(u(\delta)^{-r}-1)A = 0$, by divisibility. Thus inflation–restriction identifies degree one over D with the equivariant homomorphisms on G_L. The same local restriction at 3 is injective. Its decomposition quotient is all of $\mathrm{Gal}(L/D)$, since each finite layer has just one prime over 3. Away from 3 inertia does not change in L/D.

To see which homomorphisms occur, take a strict cocycle over D. Its image is finite by continuity and compactness. On the local decomposition group at 3 it is the coboundary of some element of A. Choose j with $F_j \supset D$ so large that G_{F_j} acts trivially on all these finitely many elements. The restriction of the cocycle to G_{F_j} is then a homomorphism unramified everywhere and zero at the prime over 3. It factors through C_j. Conversely the class fields H_jL/L are nested, with groups C_j and transition maps the norms. They realize X as a quotient of G_L. A continuous equivariant homomorphism from X to A is unramified away from 3 and zero at 3 on G_L, since it factors through some C_j. Its unique global lift is strict by the local injectivity and inertia comparison above. Equivariance means that it kills $(\delta - u(\delta)^{-r})X$. This image is compact and closed. Pontryagin duality now gives the claimed quotient. □

27.8 An exact strict order at conductor 257

Theorem 27.8 (Every positive even twist of the quadratic field)**.** *Let $K = \mathbb{Q}(\sqrt{257})$. For every positive even r, $\mathcal{S}_{3,r}(K)$ is cyclic of order three. For the primitive quadratic character of conductor 257, the full logarithmic contribution at 3 of the complementary groups fixed by $\mathrm{Gal}(E_x/K)$, summed over $1 \le r < t(x)$, is exactly $\lfloor (t(x)-1)/2 \rfloor \log 3$ on every common interval.*

Proof. The discriminant of K is 257. The real quadratic Minkowski bound $\sqrt{257}/2 < 9$ shows that the primes of norm at most eight generate the class group. The rational primes $3, 5, 7$ are inert, by the quadratic residue test. Only the two primes over 2 remain, since $257 \equiv 1 \bmod 8$. Their classes are inverses. The element $(15+\sqrt{257})/2$ has norm -8 and odd trace, so only one of these two primes divides it. Its ideal is the cube of that prime. Neither prime is principal. Indeed if z had absolute norm two, multiply it by a power of the unit $\epsilon = 16+\sqrt{257}$, of norm -1, so that in the positive embedding its absolute value u lies between $\sqrt{2/\epsilon}$ and $\sqrt{2\epsilon}$. Then $u + 2/u \le \sqrt{2\epsilon} + \sqrt{2/\epsilon} < \sqrt{257}$. The difference of the two embeddings of an algebraic integer is an integral multiple of $\sqrt{257}$. The bound forces the difference to be zero, in which case its norm is an integer square. This proves that $\mathrm{Cl}(K)$ has order three.

There is one prime over 3, and its class is principal. Since it is unramified, the global and local cyclotomic images are both $\mathbb{Z}_3^{\times}$. The finite-coefficient localization diagram in the proof of Theorem 27.5 therefore identifies $\mathcal{S}_{3,r}(K)[3]$ with $\mathrm{Hom}(\mathrm{Cl}(K), \mathbb{F}_3)$ for every even r. The same diagram over $\mathbb{Q}$ gives zero. By quadratic descent the full strict group over K is thus

its nontrivial character summand, namely the strict group over $\mathbb{Q}$ for $(\mathbb{Q}_3/\mathbb{Z}_3)(\chi\kappa_3^{-r})$, where $\chi(a) = (a/257)$ is the Legendre character. In particular this summand has an element of order three.

It remains to bound its full order. Since $\chi(3) = -1$, the residual character is nontrivial on the decomposition group at 3. Theorem 27.1 gives its length as the 3-adic valuation of the coordinate of the cyclotomic class. We evaluate this class modulo 9 at the single prime $s = 23131 = 10 \cdot 257 \cdot 9 + 1$. Take $g = 3$, $w = g^{10} = 12787 \bmod s$. Primality follows by trial division through 152. For the distinct prime divisors $2, 3, 5, 257$ of $s - 1$ the residues $g^{(s-1)/d}$ are respectively $23130, 19250, 3529, 15632$. Thus g generates $\mathbb{F}_s^\times$.

For $i \in (\mathbb{Z}/9)^\times$ put

$$B_i = \sum_{\substack{1 \le a < 2313,\ (a,2313)=1 \\ a \equiv i \bmod 9}} \chi(a)\, \mathrm{ind}_g(1 - w^a) \pmod 9.$$

Here and below ind_g is the discrete logarithm. The entries, in the displayed order, are

i	1	2	4	5	7	8
B_i	4	1	7	7	1	4

The following recurrence reproduces the table using only modular multiplication. Initialize the six entries to zero and $y = 1$. For $a = 1, \dots, 2312$, replace y by $yw \bmod s$ and skip the entry if $3 \mid a$ or $257 \mid a$. Read j from the nine-entry table $(w^{257j} \bmod s, j)$, $0 \le j < 9$, at the key $(1 - y)^{(s-1)/9} \bmod s$. Add j to $B_{a \bmod 9}$ when $a^{128} = 1 \bmod 257$, and subtract it otherwise. By the Kummer corestriction formula of Proposition 21.10, the Frobenius coordinate is $\sum_i B_i i^r \bmod 9$, up to a unit. The powers depend only on $r \bmod 6$. For $r \equiv 0, 2, 4 \bmod 6$, all three sums are $6 \bmod 9$. A class divisible by nine would evaluate to zero. Its coordinate consequently has valuation at most one, and the element of order three found above gives equality.

The fields for χ have degree a power of two over K. Restriction and averaging identify the invariant strict group with the one over K, also at all the local conditions. The odd twists have zero complementary part on the real field K. Counting even integers $1 \le r < t(x)$ proves the formula. □

27.9 Class numbers in every layer of the cyclotomic tower at three

Theorem 27.9 (An exact class group and strict group in every layer)**.** *For F_m, L, γ, X of Theorem 27.7 one has*

$$X \simeq \mathbb{Z}/9\mathbb{Z}, \qquad \gamma|_X = 1, \qquad \mathrm{Cl}(F_m)\{3\} \simeq \mathbb{Z}/9\mathbb{Z} \quad (m \ge 0).$$

All the norm maps on these primary class groups are isomorphisms. For $m \ge 1$, $\mathcal{S}_{3,r}(F_m) \simeq \mathbb{Z}/9\mathbb{Z}$ at every positive even twist. The cyclic group fixing $\mathbb{Q}(\sqrt{257})$ in F, acting on L by fixing the cyclotomic tower $Q_\infty = \bigcup_m Q_m$, acts faithfully on X. The involution σ of $F/\mathbb{Q}(\zeta_7)^+$, also extended to fix Q_∞, acts on X by inversion.

Proof. Give X its $\mathbb{Z}_3[[T]]$-module structure via $T = \gamma - 1$. The action exists on each finite norm quotient since γ has 3-power order there and T is nilpotent modulo three. The twisted quotient for $D = F$ evaluates this module at $z(r) = 4^{-r} - 1$. By Theorem 26.19, it has order three for $r = 2$ and nine for $r = 6, 12, 18$. The valuation of $z(2)$ is one. Since $4^6 \equiv 19 \bmod 27$, the values $z(6), z(12), z(18)$ are $9, 18, 0 \bmod 27$, respectively. Theorem 19.26 with $b = 2$ proves the assertions about X from these four twists.

The untwisted quotient in Theorem 27.7 is therefore X for every m. These identifications use the natural projections, so identify the norms as well. In the twisted quotient the generator is γ^{3^m}. The scalar $4^{-3^m r}$ is 1 mod 9 when $m \geq 1$. This proves the assertion about strict groups.

For the last assertion take $r = 6$, and let τ generate the cubic group in the statement. The quotient in Theorem 27.7 for $D = F$ is all of X. It identifies the action on the dual strict group with that on X, because τ can be lifted while fixing all 3-power roots of unity. Indeed F is unramified at three and is disjoint from the full 3-power cyclotomic extension. In the notation of Theorem 26.19 the same dual group is $M = H^2(U, T_R)$. Right exactness in degree two gives

$$M/(X_0 - 1)M = H^2(U, \mathbb{Z}_3(\chi\kappa_3^7)),$$

where X_0 denotes the generator in the finite cubic group ring R. This follows by factoring multiplication by $X_0 - 1$ through its image as in that theorem. The group on the right has order three, while M has order nine. Under Shapiro's identification X_0 acts by the cubic generator or its inverse, according to the choice of regular action. The class-field identification and duality commute with field automorphisms, so τ acts nontrivially on X. As it has order three it acts faithfully. In the same twist the σ-invariant strict group over F is the strict group over $\mathbb{Q}(\zeta_7)^+$, by quadratic descent, and the latter vanishes by Theorem 27.5. The lift of σ also fixes the cyclotomic coefficients. Thus the invariants on X vanish, using the integral plus projector in the dual. Since two is invertible, σ acts by -1 on all of X. □

28 Positive twists and explicit strict orders

28.1 Local conditions for the positive cyclotomic twist

Let $E = E_x$ be the abelian period field of Theorem 19.15, with cyclotomic modulus N, degree g, and $t = \lfloor x^{401} \rfloor$. Take a prime $\ell > 2t + 3$ with $\ell \nmid Ng$. Fix $1 \leq r < t$ and a character α of $\mathrm{Gal}(E/\mathbb{Q})$ with $\alpha(c) = (-1)^r$. Let $O = \mathbb{Z}_\ell[\alpha]$ denote the ring generated by its values on the Galois group. This is an unramified integer ring, with fraction field J and residue degree b_α. Write κ for the cyclotomic character and $\Psi = \alpha\kappa^r$.

Use classes over $\mathbb{Q}$ unramified away from ℓ, meaning that they restrict to zero in inertia cohomology there. Define P for $(J/O)(\Psi)$ and C for its opposite Tate twist $(J/O)(\alpha^{-1}\kappa^{1-r})$ by the following conditions at ℓ. For $r \geq 2$ allow all local classes in P and require zero in C. For $r = 1$ use Kummer classes of units in P and unramified classes in C. Here the Kummer condition is read after the unramified extension cut out locally by α, or equivalently by requiring zero valuation on inertia. Use the same conditions with finite coefficients O/ℓ^j, and denote the resulting groups by P_j, C_j.

Theorem 28.1 (The positive twist and its finite dual orders)**.** *For every $j \geq 1$,*

$$|P[\ell^j]| = |P_j| = |C_j| = |C[\ell^j]|.$$

Both modules are finite and have the same elementary divisors over O. For $r \geq 2$, C is the α-component of the strict group on E at twist $r - 1$, after extending scalars to O. For $r = 1$ it is the corresponding component of $\mathrm{Hom}(\mathrm{Cl}(E), J/O)$*, with its natural contragredient Galois action.*

Proof. The pairing of O/ℓ^j with itself induced by the unramified trace and division by ℓ^j is perfect into $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. Thus the second finite module is the Cartier dual of $M = (O/\ell^j)(\Psi)$. Away from ℓ unramified local conditions are orthogonal complements. Their cup product vanishes by inflation from the procyclic unramified quotient. Each has size equal to that of its local

invariants, by the kernel and cokernel orders of Frobenius minus one on the inertia invariants. Local duality and the local Euler characteristic formula give the complementary orders.

At ℓ and $r \geq 2$ both invariant groups vanish, since the inertia exponents $r, 1-r$ are nonzero modulo $\ell - 1$. The whole local $H^1(M)$ consequently has order $|M|$ and is orthogonal to zero. For $r = 1$, pass to the unramified extension $L/\mathbb{Q}_\ell$ killing α, of degree prime to ℓ. Restriction identifies local classes with the appropriate twisted invariants. The unit condition pairs trivially with unramified characters by local reciprocity. The logarithm on principal units identifies their pro-ℓ completion with $\ell\mathcal{O}_L$. A normal basis of the residue field lifts to an integral normal basis of $\mathcal{O}_L$, since its determinant is a unit. Taking the twisted invariants of that regular module tensored with O/ℓ^j gives one copy of O/ℓ^j. The local invariants of M vanish. The local Euler formula now gives the full orthogonal complement the size of the invariants of the dual, precisely the size of its unramified classes.

Apply finite Poitou–Tate duality and the global Euler characteristic formula in their Selmer order form. With orthogonal local conditions $L_v, L_v^\perp$, this form gives the ratio of the two Selmer orders as the ratio of the global invariant orders times $\prod_v |L_v|/|H^0(\mathbb{Q}_v, M)|$, with zero local condition at the real place. It follows by taking orders in the finite localization sequence and substituting the global Euler characteristic for the alternating product of global orders. [13, Chapter I] The global invariants vanish on both sides. For the dual at $r = 1$ this uses $\alpha(c) = -1$. The finite-place factors are one away from ℓ, and the factor at ℓ is $|M|$. Complex conjugation acts trivially on M, producing the factor $1/|M|$. This proves the middle equality.

The coefficient sequence identifies global finite classes with the ℓ^j-torsion of the divisible-coefficient cohomology, since its degree-zero invariants vanish. At inertia away from ℓ the invariants of the divisible module are either all of it or zero, as the inertial character has order prime to ℓ. They are divisible, so the finite classes inject locally on inertia. For the strict condition at ℓ in twists $r \geq 2$ the local invariants are zero. At $r = 1$ the unramified condition is detected on inertia, where the dual coefficient is trivial and divisible. On the Kummer side the valuation on the finite module embeds in the valuation on the direct limit, by naturality under $O/\ell^j \hookrightarrow J/O$. These facts give both outer equalities.

Restriction to E and the character projection identify C as stated, since g is a unit in O. In particular restriction is injective on local cohomology when tested over the corresponding local extension or inertia subgroup, by restriction followed by corestriction. For $r = 1$ the coefficient over E is constant and the everywhere unramified characters factor through the ideal class group. For $r \geq 2$ use Theorems 24.1 and 11.1; the parity at twist $r - 1$ is $(-1)^r$. In both cases C is finite. The finite-level equalities bound the increasing union forming P, so it is finite as well. The successive differences of the lengths of the ℓ^j-torsion count the elementary divisors of length at least j. This proves their equality. □

28.2 Primitive special values for the positive twist

Keep the characters, coefficient prime, and modules P, C of Theorem 28.1. Write α^* for the associated primitive Dirichlet character, of conductor f_α, using arithmetic Frobenius. Evaluate its algebraic special values at the chosen ℓ-adic embedding and normalize $v_\ell(\ell) = 1$.

Theorem 28.2 (The order in each character component)**.** *For every $1 \leq r < t$ under those hypotheses,*

$$\operatorname{length}_O P = \operatorname{length}_O C = v_\ell\big(L(1-r, \alpha^*)\big).$$

In particular the positive twist has a nonzero class precisely when the primitive value has positive valuation, including at $r = 1$ when $\alpha(\ell) = 1$.

Proof. Let K be the fixed field of the kernel of α. Its degree is prime to ℓ. Character descent in Theorem 28.1 applies equally to this field, since its proof uses only prime-to-degree restriction. The character is faithful on $G = \mathrm{Gal}(K/\mathbb{Q})$, so it is nontrivial on inertia at every ramified prime of K. The ring O is the factor of $\mathbb{Z}_\ell[G]$ obtained by evaluating at this character. We use α^{-1} when passing to a contragredient module.

First suppose $r \geq 2$. At every $w \mid \ell$ of K, the mod-ℓ cyclotomic character has full inertia image because K_w is unramified. The invariants of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(1-r)$ therefore vanish, as $0 < r-1 < \ell-1$. By local duality $H^2(K_w, \mathbb{Z}_\ell(r)) = 0$. Poitou–Tate duality as in Lemma 11.2 identifies the dual of C with the entire α^{-1}-component of $H^2(\mathcal{O}_K[1/\ell], \mathbb{Z}_\ell(r))$ after taking the coefficient factor. Inverting the primes over f_α does not change this component. The adjacent terms of the localization sequence are sums of residue-field cohomology with twist $r-1$ at these primes. Their inertia groups act trivially on the residue field and on the twist, whereas α^{-1} is ramified. Averaging over inertia kills their character components.

Apply the equivariant Coates–Sinnott equality of Greither and Popescu, in the form stated in Lemma 11.2, with the real base $\mathbb{Q}$ and the infinite and ramified places. The required cyclotomic μ-invariant vanishes by Ferrero–Washington. The group of invariants of $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)(r)$ over K vanishes by the same inertia test, now using $0 < r < \ell - 1$. The torsion factor in the equality thus has unit annihilator. The parity factor is one on α^{-1}. In that factor the zeroth Fitting ideal of the group just found is generated by $L(1-r, \alpha^*)$. Each omitted ramified Euler factor already equals one on a faithful character. If the prime ℓ is also omitted, its factor is an ℓ-adic unit. The valuation of the Fitting generator over a discrete valuation ring is the length. Duality preserves this length. [14, Theorem 6.11]

For $r = 1$ the character is odd, so K is CM. Now C is the α-component of the dual of the ordinary class group. Choose two distinct auxiliary primes away from $f_\alpha \ell$ congruent to one modulo f_α and to two modulo ℓ. They exist by Dirichlet's theorem and split completely in K. Use their set T as smoothing primes in the theorem of Dasgupta and Kakde on the Fitting ideal of the dual ray class group. Two residue characteristics satisfy the smoothing hypothesis. The ray-to-ordinary kernel is a quotient of the product of the residue unit groups at these primes, of orders prime to ℓ. The ℓ-primary modules therefore agree. Dasgupta and Kakde, *On the Brumer–Stark Conjecture*, Theorem 1.4.

For clarity, at a ramified prime q the local ideal in that formula is generated by the sum of the elements of the inertia group I_q and by $1 - \sigma_q e_q$, where e_q is their average and σ_q lifts Frobenius. Its image under α is the unit ideal, since the average has image zero. The involution on the Stickelberger factor of the dual class group makes its α-value $L(0, \alpha^*) \prod_{q \in T} (1-q)$. The smoothing factors are units. Taking the length again proves the formula. Theorem 28.1 gives the same length for P.

For example the odd quadratic character modulo 167 has $L(0, \alpha^*) = 11$. The sum of the least positive quadratic residues modulo 167, obtained by reducing the squares of $1, \dots, 83$, is 6012, and the sum of the nonresidues is 7849. Their difference in the order nonresidues minus residues is $167 \cdot 11$, giving the value by the first Bernoulli polynomial. Also 11 is a quadratic residue. Thus for this field, $r = 1$, and $\ell = 11$, the two groups have order eleven even with the unit condition at the split prime. This example uses the local hypotheses with $t = 2$. □

28.3 Every strict twist at eleven in the conductor forty-one tower

Let D be any finite subfield of $\mathbb{Q}(\zeta_{41}, \mu_{2^\infty})$. Write c for complex conjugation and use the original strict local conditions on $\mathcal{S}_{11,r}(D)$ of Section 6.4. Thus the coefficient over D is $(\mathbb{Q}_{11}/\mathbb{Z}_{11})(-r)$.

Theorem 28.3 (Vanishing on the full dyadic tower over conductor forty-one)**.** *For every such*

D and every $r \geq 1$,

$$\mathcal{S}_{11,r}(D)^{c=(-1)^r} = 0.$$

On any of the original intervals take $D_x = E_x \cap \mathbb{Q}(\zeta_{41}, \mu_{2^\infty})$. If $11 \nmid [E_x : D_x]$, the $\mathrm{Gal}(E_x/D_x)$-invariant part of the complementary strict group on E_x is zero for every twist on that interval. In particular for ψ of conductor dividing $41 \cdot 2^a$ this applies to all the classes descending to $K_\psi C_J \subset E_x$, with the actual dyadic layer C_J of the interval.

Proof. Every finite cyclotomic field used here has degree prime to eleven. The character descent of Theorem 24.1 reduces the question to $S_{\alpha,r}$ over $\mathbb{Q}$ for the primitive characters inducing its characters α with $\alpha(-1) = (-1)^r$. Its coefficient is $(J/O)(\alpha^{-1}\kappa_{11}^{-r})$, with $O = \mathbb{Z}_{11}[\alpha]$ and J its fraction field. Exactness of the character decomposition holds over the unramified coefficient integers.

First let the dyadic conductor F of α be at least 32768. In Proposition 25.16 the maximal 11-subfield is $\mathbb{Q}$. The reflected character $\omega^{r+1}\alpha$ has odd conductor $f_o \mid 11 \cdot 41$. Its odd-conductor factor has order dividing 40, since the orders of the two factors divide 10 and 40. Take $Q = 121$ in that proposition. Then $v_2(Q-1) = 3$, $40 \mid Q-1$ and $F \geq 451 \cdot 4^3$. Any extra odd prime in its Euler factors is 11 or 41, and neither is congruent to either sign of one modulo $F/8$. These verify all the hypotheses of the vanishing test.

For $F \leq 16384$ apply Theorem 28.7. It remains to treat its seven labels, each at $r \equiv 0 \bmod 10$ with $\alpha \neq 1$. Take $k = 10$ and $\chi = \alpha^{-1}$. The character $\bar{\chi}\bar{\omega}^{10} = \bar{\chi}$ is nontrivial. If the primitive value $B_{10,\chi}/10$ is a unit, the interpolation of Theorem 25.23 supplies a series $F_1 \in O[[X]]$ taking a unit value at $X_{1-10} \in 11\mathbb{Z}_{11}$. Its constant coefficient is a unit, hence so is $F_1(X_{1+r})$ for these twists. The annihilator conclusion there gives $S_{\alpha,r} = 0$.

Here are the residues of $B_{10,\chi}/10$ in the field $k_0 = \mathbb{F}_{11}[i]$ of Theorem 28.7.

F	l	e	$B_{10,\chi}/10 \bmod 11$
8	20	1	0
16	10	1	$10 + 9i$
16	30	3	$10 + 2i$
32	5	5	$9 + 8i$
32	15	7	$9 + 3i$
32	25	1	$3 + 5i$
32	35	3	$3 + 6i$

For a check using only small integers, put $M = 41F$. The generalized Bernoulli formula gives the table by summing over $1 \leq a < M$ prime to M the expression

$$\chi(a) \sum_{j=0}^{9} \tfrac{1}{10} \binom{10}{j} B_j M^{j-1} a^{10-j}.$$

The omitted constant term sums to zero since $\chi \neq 1$. The Bernoulli numbers in this sum are integral at 11, so each summand can be reduced there. The nonzero B_j in index order are $1, -1/2, 1/6, -1/30, 1/42, -1/30$, at $j = 0, 1, 2, 4, 6, 8$. For $a = 6^u \bmod 41$, $a = (-1)^b 5^v \bmod F$, use $\chi(a) = (-1)^{bl} C^{-lu} (\beta^{120e/d})^{-v}$ in k_0, where $d = F/4$. This proves vanishing in six cases. In the first case the character is the even quadratic character of conductor eight times the quadratic character of conductor forty-one. It cuts out $\mathbb{Q}(\sqrt{82})$ of discriminant 328. Theorem 28.10 proves vanishing for every positive multiple of ten in this last case as well.

This proves the assertion first for full cyclotomic layers. Restriction to a larger layer followed by corestriction is multiplication by its relative degree, prime to eleven. It follows that the

assertion holds for their subfields. For E_x/D_x of degree prime to eleven, averaging or inflation–restriction gives the isomorphism from the strict group over D_x onto the invariant subgroup over E_x. The same argument locally preserves the unramified and zero local conditions in both directions. Conjugation commutes with the isomorphism. The final assertion follows since $K_\psi C_J$ lies in the tower and the remaining extensions have degree prime to eleven for this ψ. □

As a consequence one can also read the full relaxed order on the quartic branch of Corollary 25.25. Use its $\chi(6) = i,\ r \equiv 2 \bmod 10$ and $\alpha = \chi^{-1}$. The reductions of the two moments in that corollary show that the value of its interpolation series has valuation one for every such r, since the real coordinate of its quotient by eleven is seven modulo eleven. Theorem 28.8 gives relaxed length one over $\mathbb{Z}_{11}[i]$. Its entire local image is therefore isomorphic to $\mathbb{Z}_{11}[i]/11$, of order 121, since the strict kernel has just been shown to vanish.

28.4 Testing the order of a strict group at finite level

Keep the actual field and the large prime of Theorem 34.22. Write S^- for the whole strict group with coefficient $(J/O)(\alpha^{-1}\kappa^{-r})$, and put $\beta = \alpha^{-1}$. For $j \geq 1$ define the positive weight and the integer

$$s_j = (\ell - 1)\ell^{j-1} - r, \qquad v_j = v_\ell(L(1 - s_j, \beta^*)).$$

Let K_0 be the cyclic field cut out by the residual character $\delta = \bar{\alpha}^{-1}\bar{\kappa}^{-r}$ over $\mathbb{Q}$. Let h_0 denote its ordinary class number and put $b = [O/\ell : \mathbb{F}_\ell]$.

Theorem 28.4 (Finite levels of the full complementary group)**.** *For every $j \geq 1$,*

$$\operatorname{length}_O S^-[\ell^j] \leq v_j, \qquad \dim_{O/\ell} S^-[\ell] \leq \min\left(v_1, \frac{\log h_0}{b \log \ell}\right).$$

If $v_j < j$ at one level, the full group already has length at most v_j. If its elementary divisors are written as powers of ℓ, the number of them with exponent at least j is at most $\min_{1 \leq i \leq j} \lfloor v_i/i \rfloor$.

Proof. The finite classes for $O/\ell^j(\delta_j)$, with $\delta_j = \alpha^{-1}\kappa^{-r} \bmod \ell^j$, recover $S^-[\ell^j]$ with exactly the unramified conditions away from ℓ and the zero condition at ℓ. Indeed the inertia character at ℓ has nontrivial reduction, so both the global and local divisible-coefficient invariants vanish. At every other prime the inertia action has order prime to ℓ. Averaging over its image exhibits the invariants as a direct summand of a divisible module. They are therefore divisible as well. These are the injection tests in the proof of Theorem 24.2.

Every cyclotomic unit modulo ℓ^j has exponent dividing $(\ell-1)\ell^{j-1}$. Thus this finite coefficient equals the reduction of $\beta\kappa^{s_j}$, and the strict classes inject into its positive-twist Selmer group at level j. The latter uses all local classes at ℓ. We spell out the permitted weights in applying Theorems 28.1 and 28.2 here. For weights $s \geq 2$, their finite dual-order and Fitting arguments need both s and $1 - s$ nonzero modulo $\ell - 1$. This condition kills both local invariant modules, the global torsion factor in the Coates–Sinnott formula, and the local degree-two term. Prime-to-degree character descent and the residue-field terms at ramified primes are independent of s. For $s = s_j$ the two residues are $-r, 1 + r$, both nonzero since $\ell > 2t + 3$. Also $s_j \geq 2$ and $\beta(c) = (-1)^{s_j}$. Thus the positive group over divisible coefficients has length exactly v_j, giving the asserted bound for the finite subgroup. A cyclic summand of exponent at least j contributes j to the length at level j. If $v_j < j$, there is no such summand, and $S^- = S^-[\ell^j]$. Each summand of exponent at least j contributes i at level $i \leq j$, giving the last assertion.

For the other rank bound, restriction to K_0 is injective at level one since its degree is prime to ℓ. Over this field our classes are additive homomorphisms unramified everywhere and zero

at primes above ℓ. They therefore lie in the appropriate character space of the dual class group tensored with O/ℓ. The values of δ generate O/ℓ over $\mathbb{F}_\ell$, since the residual cyclotomic factor takes its values in $\mathbb{F}_\ell^\times$. Consequently the residual character has b distinct Frobenius conjugates. They occur with equal multiplicity in a module defined over $\mathbb{F}_\ell$, and are disjoint by prime-to-degree semisimplicity. Thus b times the dimension in question is at most the $\mathbb{F}_\ell$-dimension of $\mathrm{Cl}(K_0)/\ell$, which is at most $\log h_0/\log \ell$. □

For two examples, the upper length of Theorem 28.2 is one for the trivial character at $(\ell, r) = (691, 12)$ and for the odd quadratic character of conductor 167 at $(11, 1)$. In the first case $L(-11, \mathbf{1}) = 691/32760$, and the second value is eleven as computed there. In both cases the whole complementary strict group is zero. The last column gives the test at $j = 1$.

(ℓ, r)	f_β	s_1	$B_{s_1} \bmod \ell$	$L(1-s_1, \beta^*) \bmod \ell$
$(691, 12)$	1	678	48	110
$(11, 1)$	167	9	0	3

To reproduce the entries put $u_0 = 1$ and compute $u_m = -\sum_{i<m} \binom{m+1}{i} u_i/(m+1)$ in the residue field up to $m = s_1$. All divisors are units since $s_1 < \ell - 1$. With $f = f_\beta$, multiply $\sum_{a=1}^{f} \beta^*(a) \sum_{i=0}^{s_1} \binom{s_1}{i} u_i (a/f)^{s_1 - i}$ by $-f^{s_1-1}/s_1$. For $f = 167$, $\beta^*(a)$ is the quadratic residue sign, with value zero at 167. The nonzero last entries give $v_1 = 0$ independently of the upper length.

28.5 A local correction of unbounded length at 37

Proposition 28.5 (The rational character at 37)**.** *For every positive even r the strict group over $\mathbb{Q}$ for $(\mathbb{Q}_{37}/\mathbb{Z}_{37})(-r)$ vanishes. For $r \equiv 4 \bmod 36$, let $\xi \in \mathbb{Z}_{37}$ be the zero in Proposition 21.7. When $r \neq \xi$ the group with the unrestricted condition at 37 is cyclic of order $37^{1+v_{37}(r-\xi)}$. Every positive length occurs. If $r = \xi$ is a positive integer on this branch, the group with that local condition is $\mathbb{Q}_{37}/\mathbb{Z}_{37}$.*

Proof. The strict vanishing also follows from Theorem 8.2. For a smaller calculation in this rational case use $s = 149$. The element 2 generates $\mathbb{F}_{149}^\times$, since $2^{74} = -1 \bmod 149$ and $2^4 \neq 1 \bmod 149$. Put $w = 2^4 = 16$. For $1 \le a \le 36$ take $j_a \bmod 37$ with $2^{j'} = 1 - w^a \bmod 149$ and $j_a = j' \bmod 37$. The following are the moments $D_r = \sum_{a=1}^{36} a^r j_a \bmod 37$.

r	0	2	4	6	8	10	12	14	16
D_r	35	3	26	35	25	23	26	3	6
r	18	20	22	24	26	28	30	32	34
D_r	29	16	18	13	16	32	35	33	29

For a direct reproduction, enumerate $2^i \bmod 149$ for $0 \le i < 148$, recording $i \bmod 37$ at the corresponding residue. Start at $z = 1$. For each $a = 1, \dots, 36$ replace z by $16z \bmod 149$, read the recorded entry at $1 - z$, and add it times a^r modulo 37. This is exactly the split-prime Kummer formula of Proposition 9.5 at precision one and conductor one. Every entry is nonzero, also for the residue of positive multiples of 36. That proposition and Theorem 27.1 give vanishing of the strict group. The moments have period 36 in r.

On the indicated irregular branch take $B = 2$ in Theorem 28.8. Proposition 21.7 calculates $v_{37}(F(X_{1+r})) = 1 + v_{37}(r - \xi)$. With $S = 0$ the entire relaxed group is its image in the local line, giving the two assertions about that group. For each $j \ge 0$ choose a residue modulo 37^{j+1} at distance 37^{-j} from ξ. The Chinese remainder theorem supplies a positive r in that residue with $r = 4 \bmod 36$. □

Whenever $37 \nmid [E_x : \mathbb{Q}]$, character descent in Theorem 24.1 identifies the same vanishing group with the trivial-character summand over the period field.

28.6 Positive twists with a ramified or exceptional local character

Let p be odd and let γ be a primitive Dirichlet character of order prime to p, of conductor f. The prime p may divide f. Write $O = \mathbb{Z}_p[\gamma]$, $J = \operatorname{Frac} O$, $\kappa = \kappa_p$, and let ω be its Teichmüller part. For a discrete coefficient with this finite character part, write R for cohomology classes of degree one over $\mathbb{Q}$ unramified at every finite prime away from p, with all local classes allowed at p.

Theorem 28.6 (The relaxed positive twist at every tame local type)**.** *For $k \geq 2$, $\gamma(-1) = (-1)^k$, and $\bar{\gamma}\bar{\omega}^k \neq 1$ as a global character,*

$$\operatorname{length}_O R((J/O)(\gamma\kappa^k)) = v_p(L(1-k,\gamma)).$$

If $\bar{\gamma}\bar{\omega}^m = 1$ globally for a nonzero integer m, then $R((J/O)(\gamma\kappa^m)) = 0$. This includes negative m.

Proof. Write $T_k = O(\gamma\kappa^k)$, $V_k = T_k \otimes_O J$ and $U = \operatorname{Spec} \mathbb{Z}[1/fp]$. At every $q \mid f$ other than p, inertia acts nontrivially, of order prime to p, on both the coefficient modulo p^j and its Cartier dual. Their invariants vanish. The local Euler characteristic and local duality at $q \neq p$ give vanishing of both groups in degree one. Taking the direct limit shows that $R = H^1(U, V_k/T_k)$.

Take L to be the compositum of the field cut out by γ with $\mathbb{Q}(\mu_p)$. This abelian CM extension has degree prime to p and is unramified outside fp. Over L the finite character becomes trivial. The rational degree-two group of the positive twist is zero by the comparison with the finite even K-group of the ring of integers. Inverting additional primes preserves this vanishing since the residue-field terms are finite for $k \geq 2$. Averaging descends the vanishing to $H^2(U, V_k)$. Also $H^0(U, V_k) = 0$ since the cyclotomic power has infinite image. The global Euler characteristic of V_k over $\mathbb{Q}$ is minus the dimension of its odd subspace, here zero. Consequently $H^1(U, V_k) = 0$, and the coefficient sequence identifies R with $H^2(U, T_k)$.

Averaging identifies $H^2(U, T_k)$ with the γ^{-1}-factor of degree two over L with coefficient $\mathbb{Z}_p(k)$, extended to O. Use the refined Coates–Sinnott equality of Greither and Popescu with the infinite places and the primes dividing fp. The cyclotomic μ-invariant vanishes by Ferrero–Washington since $L/\mathbb{Q}$ is abelian. In the selected factor the torsion in integral degree one is $H^0(\mathbb{Q}, V_k/T_k)$, by the coefficient sequence and the same descent. It vanishes because the global residual character is nontrivial. Its annihilator is therefore the unit ideal. The parity idempotent acts as the identity. The resulting zeroth Fitting ideal of $H^2(U, T_k)$ is generated by the primitive value $L(1-k,\gamma)$ up to a unit. At $q \mid f$ the primitive Euler factor is already one. At $p \nmid f$ the removed factor $1 - \gamma(p)p^{k-1}$ is a unit. The valuation of a zeroth Fitting generator over O is the length. Greither and Popescu, *An equivariant main conjecture in Iwasawa theory and applications*, Theorem 6.11.

In the last assertion reduction on roots of unity of order prime to p is injective. Thus $\gamma = \omega^{-m}$, $O = \mathbb{Z}_p$, and $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\langle\kappa\rangle^m)$ is unramified outside p. Its global invariants have order $p^{1+v_p(m)}$ because $1 + p$ generates the principal units topologically. The global multiplication sequence injects $A^{G_\mathbb{Q}}/pA^{G_\mathbb{Q}}$ into $H^1(\mathbb{Z}[1/p], A[p])$, with cokernel $R(A)[p]$. Here $A[p]$ is trivial, and the middle group is one-dimensional over $\mathbb{F}_p$. Indeed its characters factor through the maximal abelian extension of $\mathbb{Q}$ unramified away from p, whose pro-p quotient is $1 + p\mathbb{Z}_p$ by Kronecker–Weber. The injection from the group of order p fills it. Every nonzero p-primary group has an element of order p, so $R(A) = 0$. □

28.7 Two residue computations at eleven for conductor forty-one

Work in $k = \mathbb{F}_{11}[i]$, with $i^2 = -1$. The powers of $\beta = 1 + 4i$ with exponents $24, 40, 60$ are $3, 5+3i, -1$, so β generates $k^\times$. Write $C = \beta^3$, of order forty. The element 6 generates $(\mathbb{Z}/41)^\times$, since $6^8 = 10$ and $6^{20} = -1 \bmod 41$. For a primitive character α with odd conductor $f = 1$ or 41, use $0 \le l < 40$ for the exponent such that its odd-conductor factor at 6 reduces to C^l. Thus $f = 1$ precisely for $l = 0$. Let F denote its dyadic conductor, and put $r_0 = r \bmod 10$ in $\{0, \dots, 9\}$. We always impose $\alpha(-1) = (-1)^r$.

If $F \ge 8$, put $d = F/4$, $m = \max(1, d/8)$ and $D = d/m$. The dyadic character at 5 has reduction Y of order d. Specify it up to Frobenius over k by an odd $e \in [1, D)$ with $Y^m = \beta^{120e/D}$. For $F = 1, 4$ put $d = m = D = 1$, $e = 0$, $Y = 1$. At $F = 1$ admissibility requires $l + r_0$ even, and at $F = 4$ it requires $l + r_0$ odd. At $F \ge 8$ the value of the dyadic character at -1 is fixed by this same parity and imposes no other condition on l, r_0.

Theorem 28.7 (Finite-field tests through dyadic conductor 16384)**.** *For $F \le 16384$ and every $r \ge 1$ of the prescribed parity, the strict group $S_{\alpha,r}$ at 11 with coefficient $(J/O)(\alpha^{-1}\kappa_{11}^{-r})$ over $\mathbb{Q}$ vanishes outside the labels in this table at $r_0 = 0$.*

F	(l, e)
8	$(20, 1)$
16	$(10, 1)$, $(30, 3)$
32	$(5, 5)$, $(15, 7)$, $(25, 1)$, $(35, 3)$.

Proof. Use the cyclotomic moment of Proposition 9.5 at precision one. Its hypotheses hold since $11 \nmid fF\varphi(fF)$. A nonzero value proves vanishing of the full strict group for every positive r in that residue class. We give the finite calculations explicitly. The two auxiliary primes s, with a generator g of $\mathbb{F}_s^\times$, are

$$(140394497, 3), \qquad (177340417, 5).$$

They have $s - 1 = 19 \cdot 451 \cdot 2^{14}$ and $s - 1 = 24 \cdot 451 \cdot 2^{14}$, respectively. Primality is checked by trial division through $\lfloor \sqrt{s} \rfloor$. The powers $g^{(s-1)/q}$ for the distinct prime divisors $q \mid s - 1$, in increasing order, are $140394496, 84793338, 132557353, 109523072$ in the first case and $177340416, 168997293, 28977015, 148801780$ in the second.

For $F \ge 8$, the odd residue classes modulo F are $(-1)^b 5^v$ for $b = 0, 1$ and $0 \le v < d$. Indeed $v_2(5^{2^j} - 1) = j + 2$ by successive squaring, so the subgroup generated by 5 consists of the classes equal to one modulo four. A primitive character has order d at 5, since $5^{d/2} = 1 + F/2 \bmod F$. If $d > 8$, the order of 121 modulo d is $d/8$, since $v_2(121^{2^a} - 1) = 3 + a$ for all $a \ge 0$. Thus the minimal polynomial over k of each possible Y is $Z^m - \eta$, where $\eta = \beta^{120e/D}$. Indeed it divides this polynomial and has degree m. For $d \le 8$ the same description with $m = 1$ follows from $d \mid 120$.

Put $w = g^{(s-1)/(11fF)} \bmod s$. For $1 \le a < 11fF$ prime to $11fF$, define $L(a)$ as the unique integer $0 \le L < 11$ for which

$$(1 - w^a)^{(s-1)/11} = g^{L(s-1)/11} \pmod{s}.$$

Write $a = (-1)^b 5^v \bmod F$ and $a = 6^j \bmod 41$ for the respective coordinates. Set $j = 0$ at $f = 1$. At $F = 4$ use $v = 0$, and at $F = 1$ use $b = v = 0$. The moment at Y is the value of the polynomial whose coefficient of Z^v is the sum of $(-1)^{b(l+r_0)} C^{lj} a^{r_0} L(a)$ over these a. After reduction modulo $Z^m - \eta$, a nonzero coefficient proves nonvanishing at every root in that orbit.

For reproducibility the following are the full counts of labels left after testing the coefficients with indices $0 \le k_0 < \min(m, 3)$. The last column is cumulative. The last row applies to each of the nine separate conductors $64, 128, \dots, 16384$.

F	admissible labels	$s = 140394497$	both primes
1	200	5	0
4	200	8	0
8	400	13	1
16	800	8	2
32	1600	16	4
$64, \dots, 16384$	1600	0	0

Here are direct recurrences to reproduce the counts and surviving labels with integer arithmetic. Start an accumulator in k at zero for each s, F, l, e, r_0, k_0. Loop over $0 \le q < D$ and set $v = k_0 + mq$. For each admissible sign b, each $0 \le j < 40$ (just $j = 0$ at $f = 1$), and $1 \le t \le 10$, take by the Chinese remainder theorem

$$a \equiv (-1)^b 5^v \bmod F, \quad a \equiv 6^j \bmod f, \quad a \equiv t \bmod 11.$$

Use just $b = 0$ for $F = 1$ and both signs for $F \ge 4$. Add $\eta^q (-1)^{b(l+r_0)} C^{lj} t^{r_0} L(a)$. In this recurrence multiplication of coordinate pairs is $(a, b)(c, d) = (ac - bd, ad + bc) \bmod 11$. Discard a label as soon as one accumulator is nonzero. The labels remaining in the last column are exactly those displayed in the statement. This computes selected coefficients sufficient for every vanishing claimed here. □

28.8 The local correction to the interpolated order

Let $E/\mathbb{Q}$ be one of the abelian period fields, of degree n and cyclotomic modulus N. Let p be an odd prime with $p \nmid nN$, and let $r \ge 1$ satisfy $r \not\equiv 0, -1 \bmod (p-1)$. Take a character α of $\mathrm{Gal}(E/\mathbb{Q})$ with $\alpha(-1) = (-1)^r$. Use its primitive character of conductor f, and write $\beta = \alpha^{-1}$, $O = \mathbb{Z}_p[\alpha]$, $J = \mathrm{Frac}\, O$. Write κ for the cyclotomic character. The two coefficients are

$$A = (J/O)(\beta \kappa^{-r}), \qquad T = O(\alpha \kappa^{r+1}).$$

In $H^1(\mathbb{Q}, A)$ let R consist of classes unramified at every finite prime other than p, and let S be the kernel of localization at p on R. Write U_T for the compact group of classes for T unramified away from p.

Choose $B > 1$ prime to fp with $\beta(B) B^{-r} \ne 1 \bmod p$. Such a residue exists by varying $B \bmod p$ with $B = 1 \bmod f$. Put $X_z = (1+p)^z - 1$ for $z \in \mathbb{Z}_p$ and $h = r + 1 \bmod (p-1)$. We use the integral series F of Lemma 25.18, normalized by $F(X_z) = A_B(z)$ there. More explicitly, on $(\mathbb{Z}/f)^\times \times \mathbb{Z}_p^\times$ integrate $\beta(a)\omega(a_p)^{-h}(1+X)^{-\log\langle a_p\rangle/\log(1+p)}$ against its bounded measure with cylinder weights $\lfloor Ba/(fp^j) \rfloor - (B-1)/2$. Here ω is the Teichmüller character and $\langle a_p \rangle = a_p/\omega(a_p)$. The binomial coefficients are integral, giving $F \in O[[X]]$. Formula (25.14) gives, for $k \ge 2$ with $k \equiv -r \bmod (p-1)$,

$$v_p(F(X_{1-k})) = v_p(L(1-k, \beta)).$$

We normalize $v_p(p) = 1$ and put $v_p(0) = +\infty$.

Theorem 28.8 (Order of the relaxed group and the strict local correction)**.** *Both U_T and $H^1(\mathbb{Q}_p, T)$ are free O-modules of rank one. Write localization between bases as multiplication by $\rho \in O$, and put $\lambda = \mathrm{length}_O S$. Then*

$$(F(X_{r+1})) = (p^\lambda \rho) \quad \textit{as ideals of } O.$$

If the value is nonzero, R is finite of length $v_p(F(X_{r+1}))$ and R/S is cyclic of length $v_p(\rho)$. If the value is zero, then $\rho = 0$ and $R/S \simeq J/O$. When $p \nmid f\varphi(f)$, the same ideal is generated by the local coordinate of the cyclotomic class $c_{\alpha,r+1}$ of Theorem 27.1.

Proof. For large j put $k_j = (p-1)p^{j-1} - r \geq 2$. The characters $\beta\kappa^{k_j}$ and $\beta\kappa^{-r}$ agree modulo p^j. With either divisible coefficient, its global invariants vanish by the inertia action at p. At other inertia groups the invariants are divisible since averaging over the finite image of order prime to p projects onto them. The multiplication sequence for p^j therefore recovers the same group $R[p^j]$ from the finite coefficient with unramified conditions away from p and unrestricted condition at p.

For the positive weight k_j this finite group is the p^j-torsion of a finite module of length $v_j = v_p(L(1-k_j, \beta))$. Indeed the proof of Theorem 28.4 applies with $k_j, 1-k_j$ nonzero modulo $p-1$. The field cut out by β has degree prime to p and is unramified at p. These are the descent and local hypotheses of Theorems 28.1 and 28.2 in weights at least two. Now $X_{1-k_j} \equiv X_{1+r} \bmod p^j$, by the binomial theorem. If $w = v_p(F(X_{1+r})) < \infty$, we have $v_j = w < j$ for all sufficiently large j. A module of length w is then killed by p^j. Thus $R[p^j]$ has length w for all these j. The nested groups exhaust R, proving its order. If $F(X_{1+r}) = 0$, then $v_j \geq j$. The p^j-torsion of a finite module of length at least j has length at least j, by its elementary divisors. Hence R is infinite in this case.

At $q \mid f$ inertia acts nontrivially through a group of order prime to p on T/p^j and its Cartier dual. Both groups of invariants vanish. Local duality and the Euler characteristic at $q \neq p$ then give zero in degree one for both coefficients. Consequently $U_T = H^1(\operatorname{Spec}\mathbb{Z}[1/fp], T)$. Its rank is one by Theorem 27.3. In detail, its rational degree two is zero by descent to the finite even K-group, its degree zero vanishes, and its rational Euler characteristic is minus one since T is odd. The absence of invariants modulo p gives torsion freeness. For the local group the two residual inertia characters ω^{-r} and ω^{r+1} are nontrivial. The multiplication sequence, local duality and the Euler characteristic over $\mathbb{Q}_p$ give a torsion-free module of rank one in degree one. Its dual $H^1(\mathbb{Q}_p, A)$ identifies with J/O using the unramified trace pairing.

The annihilator of the image of R in $H^1(\mathbb{Q}_p, A)$ is the localization of U_T. To see this first use finite Poitou–Tate duality for $A[p^j]$ and T/p^j, with the unramified conditions away from p, which are exact orthogonal complements by the local calculation in Theorem 28.1. The image at p for one coefficient is the orthogonal complement of the image for the other. If a local integral class annihilates R, at every j its reduction therefore has a global lift with the required conditions. Those sets of lifts are finite. Reduction carries higher lifts to lower lifts, so every finite list of levels admits compatible lifts by starting at the largest. Compactness gives a compatible lift at all levels, which belongs to U_T. The other inclusion follows from the same finite pairings. This proves the annihilator assertion. See Milne, *Arithmetic Duality Theorems*, Chapter I, Sections 2 and 4.

The image in J/O is therefore $(J/O)[\rho]$. The kernel S is finite by Theorems 25.1 and 24.1. If R is finite, taking lengths proves $w = \lambda + v_p(\rho)$. If R is infinite, its image is infinite and $\rho = 0$. This proves the ideal equality in both cases. Finally Theorem 27.1 writes the cyclotomic class as an O-basis of U_T times a scalar of valuation λ, since $r \not\equiv 0 \bmod (p-1)$ kills both invariant terms in its formula. Localization gives the last assertion. □

28.9 Removing the factor forced by local torsion

Keep $r \geq 1$, $A = (J/O)(\alpha^{-1}\kappa^{-r})$, $T = O(\alpha\kappa^{r+1})$, and $\alpha(-1) = (-1)^r$. Assume only that p is odd and the order of α is prime to p. Write $\alpha = \alpha_0\omega^a$ with α_0 of conductor prime to p. This is the character decomposition on the two factors of the modulus. The factor at p is

tame since its order is prime to p. If the global residual character of A is trivial, Theorem 28.6 already gives $R = S = 0$. Otherwise take the integral series F of Theorem 25.23 for the branch $k \equiv -r \bmod (p-1)$, using the primitive character α^{-1}. Its unit smoothing factor and interpolation hold also when p divides the conductor. Put

$$e = \begin{cases} 1 & a + r + 1 \equiv 0 \bmod (p-1) \text{ and } \alpha_0(p) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 28.9 (An integral factor and the full strict order)**.** *The series $F^\circ(X) = F(X)/X^e$ belongs to $O[[X]]$. The compact global group U_T is free of rank one. Let ρ represent its localization in the free quotient of $H^1(\mathbb{Q}_p, T)$, in integral bases. For $\lambda = \operatorname{length}_O S$,*

$$(F^\circ(X_{1+r})) = (p^\lambda \rho).$$

At a positive sample $k \geq 2$ on the branch one has

$$v_p(F^\circ(X_{1-k})) = v_p(L(1-k, \alpha^{-1})) - e(1 + v_p(k-1)) \ \geq 0.$$

If this number is zero at one sample, the strict group vanishes for every positive twist on the branch. The relaxed group at each of these twists is cyclic of length $e(1 + v_p(r+1))$.

Proof. Take $k_j = (p-1)p^{j-1} - r$ for sufficiently large j. The residual character at this positive weight is the same nontrivial global character. The finite level argument in Theorem 28.8 identifies $R[p^j]$ with the p^j-torsion of the positive relaxed group. It uses global residual nontriviality and divisibility of invariants at inertia away from p, with no condition at p. Theorem 28.6 gives the positive group length $v_p(F(X_{1-k_j}))$. Since $X_{1-k_j} = X_{1+r} \bmod p^j$, the same nested-group argument proves that R has length $v_p(F(X_{1+r}))$ if this is finite, and is infinite otherwise.

The global line and the local orthogonality calculation in Theorem 28.8 still apply. To check the latter when local invariants occur, use the finite local pairings and pass to the compact inverse limit on the T side. An integral class pairs with finite classes through its reduction, irrespective of the kernel of the map to local divisible coefficients. The finite lifting and compactness argument there gives the annihilator of the image of R exactly as before. Thus, writing $H = H^1(\mathbb{Q}_p, T)$, the dual of R/S is $H/\operatorname{loc} U_T$. Finiteness of S follows by restriction to the compositum of the field cut out by α and $\mathbb{Q}(\mu_p)$. Its degree is prime to p, so restriction is injective by corestriction. Over this field finiteness follows from the even K-group comparison of Theorem 25.1.

Rationally H has rank one by the local Euler characteristic, since both nonzero cyclotomic powers have zero rational invariants. Its torsion is $H^0(\mathbb{Q}_p, (T \otimes_O J)/T)$. The inertia character there is $\omega^{a+r+1}\langle\kappa\rangle^{r+1}$. A Frobenius lift fixing the local cyclotomic extension acts by $\alpha_0(p)$. Such a lift exists since that extension is totally ramified. If either residual factor is nontrivial, the invariants are zero. Otherwise their order as an O-module is determined by $v_p((1+p)^{r+1} - 1) = 1 + v_p(r+1)$. Thus the torsion is cyclic of length $\tau = e(1 + v_p(r+1))$. When $\rho \neq 0$ the torsion injects into $H/\operatorname{loc} U_T$ with quotient $O/\rho O$. When $\rho = 0$ that quotient of H has positive rank. Together with finiteness of S this proves

$$(F(X_{1+r})) = (p^{\lambda+\tau}\rho).$$

If $e = 1$, choose positive integers r_i on the same branch with $r_i + 1 = 0 \bmod p^i$, using the Chinese remainder theorem. The preceding equality gives $F(X_{1+r_i}) \in p^{i+1}O$, while $X_{1+r_i} \to 0$. Continuity gives $F(0) = 0$. Division by X is then integral. At every nonzero integer z, $v_p(X_z) = 1 + v_p(z)$, proving both formulas. An integral series taking a unit value at one point

of pO has unit constant term and takes unit values everywhere on pO. In that case $\lambda = 0$ and ρ is a unit, so $H/\operatorname{loc} U_T$ is its cyclic torsion subgroup up to isomorphism. This proves the last assertion. □

For example take $p = 3$ and the primitive character $\alpha = \chi_{-8}$ of conductor eight. It is odd and $\alpha(3) = 1$, so $e = 1$ on every odd twist. The residual character is nontrivial on inertia at two. At $k = 3$ the values of α on $1, 3, 5, 7$ are $1, 1, -1, -1$. With $B_3(u) = u^3 - 3u^2/2 + u/2$, the expression $-8^2 \sum_b \alpha(b) B_3(b/8)/3$ gives $L(-2, \alpha) = -3$. The corrected valuation is $1 - (1 + v_3(2)) = 0$. For every positive odd r the strict group vanishes and the relaxed group has order exactly $3^{1+v_3(r+1)}$.

28.10 A split uniformizer test for strict quadratic classes

Let $D/\mathbb{Q}$ be real quadratic, α its quadratic character, and p an odd split prime with primes $w, \bar{w}$ in D. Identify both completions with $\mathbb{Q}_p$. For $z \in \mathbb{Q}_p^\times$ set

$$l_p(z) = \frac{(zp^{-v_p(z)})^{p-1} - 1}{p} \pmod{p}.$$

This additive-valued homomorphism is zero on p and generates the one-dimensional space of $\mathbb{F}_p$-valued characters of the units. Indeed it is nonzero at $1 + p$, trivial on the prime-to-p roots of unity, and zero on $1 + p^2\mathbb{Z}_p$.

Theorem 28.10 (Vanishing from a split principal-ideal relation)**.** *Assume that the quotient of the class group of D by the classes of $w, \bar{w}$ has order prime to p. Suppose there is an element $z \in \mathcal{O}_D[1/p]^\times$ with $l_p(z_w) \neq l_p(z_{\bar{w}})$. For every positive $r \equiv 0 \bmod (p-1)$ the entire strict group over $\mathbb{Q}$ with coefficient $A = (\mathbb{Q}_p/\mathbb{Z}_p)(\alpha\kappa_p^{-r})$ is zero. In particular this holds for $D = \mathbb{Q}(\sqrt{82})$ and $p = 11$.*

Proof. The residual character of A is α, which is nontrivial. Hence $A^{G_\mathbb{Q}} = 0$ and the multiplication-by-p sequence identifies a global class killed by p with a unique class with coefficients in $A[p]$. On restriction to D this becomes an additive character into $\mathbb{F}_p$. Restriction is injective since $[D : \mathbb{Q}] = 2$ is prime to p. The character changes sign under the nonidentity element of $\mathrm{Gal}(D/\mathbb{Q})$. It is unramified away from p. Indeed there the original strict class is unramified over D, and inertia acts trivially on the divisible module A over D. On inertia the map in degree one from $A[p]$ to A is injective by the multiplication sequence.

At a place of D above p the original class is zero. Its finite-coefficient character is therefore a boundary of a local invariant $a \in A^{G_{\mathbb{Q}_p}}$. On choosing y with $py = a$, its cocycle is $(\kappa_p(g)^{-r} - 1)y$. Local reciprocity sends p to an element acting trivially on all p-power roots of unity. Indeed p is the norm of $1 - \zeta_{p^j}$ in each of the local cyclotomic extensions. The local character thus kills p. On identifying the two local fields, their characters are $t\, l_p$ and $-t\, l_p$ for a single $t \in \mathbb{F}_p$, by the sign under quadratic conjugation. Global reciprocity on the principal idele z gives

$$t(l_p(z_w) - l_p(z_{\bar{w}})) = 0.$$

The other finite components are units, and the archimedean components contribute zero for odd p. The hypothesis forces $t = 0$. The character is now everywhere unramified and trivial on both primes over p. It factors through the class-group quotient in the statement and so vanishes. A nonzero element of a p-primary torsion group would have a multiple of order p. This proves the assertion at all orders.

For the example, $\mathcal{O}_D = \mathbb{Z}[\sqrt{82}]$ has discriminant 328, and the two roots of $X^2 - 82$ modulo 121 are $18, -18$. Minkowski's bound $\sqrt{328}/2 < 10$ shows that prime ideals of norm less than

ten generate the class group. The primes $5, 7$ are inert, since 82 is a nonsquare modulo each, so only primes over $2, 3$ are needed. The prime $\mathfrak{q}$ above 2 is ramified, and 3 splits. The element $8 + \sqrt{82}$ has norm -18 and is not divisible by the ideal (3). Its ideal is therefore $\mathfrak{q}\mathfrak{r}^2$ for one prime $\mathfrak{r}$ over 3. The other prime over 3 has inverse ideal class. Since $[\mathfrak{q}]^2 = 1$, this proves that the class group has exponent dividing four.

Take $z = 203 + 18\sqrt{82}$, of norm $14641 = 11^4$. At the embedding with $\sqrt{82} \equiv 18 \bmod 121$, $z_w \equiv 43 \bmod 121$ and $43^{10} \equiv 45 \bmod 121$. Thus $l_{11}(z_w) = 4$. Since $z_{\bar{w}}/11^4 = 1/z_w$, the value at the other prime is -4. Their difference is nonzero modulo eleven. □

28.11 Local cyclotomic degrees and ordinary class groups

Let $F/\mathbb{Q}$ be abelian and p odd. At each $w \mid p$ local reciprocity followed by the principal cyclotomic character gives a homomorphism $\lambda_w : F_w^\times \to \Gamma_w \subseteq \Gamma_F$. Use additive coordinates on the procyclic groups. The image is all of Γ_w. Indeed local reciprocity has dense image, and the image of a sufficiently deep principal unit group contains an open subgroup. This last assertion follows also from the trace formula for the logarithm of the local norm, since the trace of a full lattice contains a nonzero ideal of $\mathbb{Z}_p$. Put

$$Z = \bigoplus_{w \mid p} \Gamma_w, \qquad I = \sum_{w \mid p} \Gamma_w \subseteq \Gamma_F, \qquad Z^0 = \ker(Z \xrightarrow{\sum} I).$$

Write $C = \mathrm{Cl}(\mathcal{O}_F[1/p])\{p\}$ for the p-part of the ordinary class group after inverting p, and $\lambda = (\lambda_w)_{w \mid p}$ on the p-units.

Theorem 28.11 (The integral contribution from the local degrees)**.** *There is a surjection $C \to \Gamma_F/I$ and an exact sequence*

$$0 \longrightarrow Z^0/\overline{\lambda(\mathcal{O}_F[1/p]^\times)} \longrightarrow \widetilde{C}(F) \longrightarrow \ker(C \to \Gamma_F/I) \longrightarrow 0.$$

Let s be the number of places over p. Take $s - 1$ independent columns of logarithms of p-units in a $\mathbb{Z}_p$-basis of Z^0, forming a square matrix B. Such a list exists. Put $a_B = v_p(\det B)$ and let e_B be the largest exponent among its Smith elementary divisors. For $s = 1$ take both numbers zero. Then

$$\log_p |\widetilde{C}(F)| \le a_B + \log_p |C| - \log_p [\Gamma_F : I], \qquad \log_p \exp \widetilde{C}(F) \le e_B + \log_p \exp C.$$

Here exp *of a finite group denotes its exponent, with value one for the trivial group.*

Proof. At depth n, quotient the ideles by the principal ideles, the infinite factors, the units away from p, and the inverse images of $p^n\Gamma_w$ under λ_w at the places over p. The result is a finite abelian group. Indeed quotienting further by Z/p^nZ gives the ordinary class group after inverting p. Its local kernel is the image of Z/p^nZ, and the only relations there are the logarithms of the p-units. To verify the last statement, a principal idele representing a tuple supported over p modulo the other local factors has valuation zero at every prime away from p. Its generator is a p-unit. Conversely such a generator gives the stated relation. Local surjectivity gives all of Z/p^nZ before imposing principal relations.

Take the p-primary parts and pass to the inverse limit in n. Finite abelian primary decomposition is exact, and the transition maps on the local quotients are onto. Global reciprocity identifies the middle limit with $X(F)$, since every finite abelian p-quotient with these local conditions factors through one of the displayed depths. On Z the kernel in the limit is the closure of the subgroup generated by the p-units, by reduction modulo each p^n. The map $X(F) \to \Gamma_F$ is surjective and acts on the local factors by their sum. Principal relations lie in

Z^0 by reciprocity. This induces the asserted surjection from C. A class in its kernel can be lifted to $X(F)$ and its degree in I cancelled by a local tuple. The remaining kernel consists exactly of the degree-zero local tuples modulo the principal relations, which proves exactness.

Finiteness of the middle group for this abelian field gives finite index for the closed logarithm subgroup in Z^0. This free module has rank $s-1$, since I has rank one. The logarithms therefore span over $\mathbb{Q}_p$ and contain the required independent list. The lattice spanned by the selected columns has index p^{a_B}, and its quotient has exponent p^{e_B} by Smith reduction. The same bounds hold after adjoining the remaining logarithms. The order formula and multiplication of the two annihilators in the exact sequence prove the two inequalities. □

28.12 An exact split contribution of order nine

Let $D = \mathbb{Q}(\sqrt{5611})$. Since $5611 = 31 \cdot 181$ is squarefree and congruent to three modulo four, the integer ring is $\mathbb{Z}[\sqrt{5611}]$ and the fundamental discriminant is 22444. The prime three splits into two primes $w, \bar{w}$. The following computation measures the local logarithms at both primes.

Theorem 28.12 (A split quadratic component on the prime-count fields)**.** *For every positive multiple r of 18, $\mathcal{S}_{3,r}(D) \simeq \mathbb{Z}/9$. For every positive even r the group is cyclic and has order at least three. For $6 \mid r$ it has order at least nine. For the primitive quadratic character of conductor 22444, the complementary groups over E_x fixed by $\mathrm{Gal}(E_x/D)$ therefore have total logarithmic order on the twists divisible by 18 equal to*

$$\left\lfloor \frac{t(x)-1}{18} \right\rfloor \log 9$$

on every common interval. Summing over all $1 \le r < t(x)$ gives a lower bound $(\lfloor (t(x)-1)/2 \rfloor + \lfloor (t(x)-1)/6 \rfloor) \log 3$.

Proof. First $\mathrm{Cl}(\mathcal{O}_D[1/3])\{3\} = 0$. Indeed the Minkowski bound is $\sqrt{5611} < 75$. Among odd primes less than 75, apart from 3 and the ramified prime 31, the split primes are

$$5,\ 7,\ 11,\ 17,\ 19,\ 43,\ 47,\ 53,\ 61,\ 71.$$

This is checked by squaring residues modulo those primes and testing the other primes $13, 23, 29, 37, 41, 59, 67, 73$. The prime two is ramified. Inert primes are principal, and ramified prime classes have order dividing two. For each split prime its two classes are inverses. The rows of the table are ordered so that its listed prime is the only new split prime away from three in the norm.

q	a	$\lvert a^2 - 5611 \rvert$	q	a	$\lvert a^2 - 5611 \rvert$
7	75	$2 \cdot 7$	5	74	$3^3 \cdot 5$
61	72	$7 \cdot 61$	43	8	$3 \cdot 43^2$
47	73	$2 \cdot 3 \cdot 47$	17	69	$2 \cdot 5^2 \cdot 17$
19	62	$3 \cdot 19 \cdot 31$	11	56	$3^2 \cdot 5^2 \cdot 11$
53	24	$5 \cdot 19 \cdot 53$	71	12	$7 \cdot 11 \cdot 71$

For each odd split prime in a norm only one of the two primes divides $a + \sqrt{5611}$, since the two residue roots are distinct. Each new exponent is a unit modulo three. Reading the rows from left to right therefore kills the class of each listed prime modulo three. Minkowski's bound gives the assertion.

The fundamental unit is $\varepsilon = 11954870 + 159597\sqrt{5611}$. For verification the continued fraction of $\sqrt{5611}$ has initial entry 74 and period

$$1, 9, 1, 2, 2, 2, 1, 1, 1, 2, 2, 2, 1, 9, 1, 148.$$

These entries follow from $m' = da - m$, $d' = (5611 - (m')^2)/d$, $a' = \lfloor (74 + m')/d' \rfloor$ starting with $m = 0, d = 1, a = 74$. The convergent just before the last period entry yields the displayed unit by the continued-fraction theorem for Pell's equation. Norm -1 is impossible modulo four. The element $z = 149 + 2\sqrt{5611}$ has norm $-243 = -3^5$. At one prime over three it is a unit. The valuation vectors of $3, z$ at the two primes consequently generate a lattice of index five in $\mathbb{Z}^2$. Together with $-1, \varepsilon$ they generate a subgroup of the 3-units of index dividing five. Indeed the kernel of the valuation map is the ordinary unit group.

Both completions are $\mathbb{Q}_3$. Identify local cyclotomic degree with the logarithm of the unit part divided by $\log 4$, up to the common reciprocity sign. The uniformizer 3 has degree zero. Both local images equal $\Gamma_D = 1 + 3\mathbb{Z}_3$, written additively in this coordinate. Thus Z^0 in Theorem 28.11 consists of pairs $(a, -a)$. At a unit u the coordinate has valuation $v_3(u^2 - 1) - 1$, since log preserves valuation on $1 + 3\mathbb{Z}_3$. The two roots of 5611 modulo 81 are $47, -47$. At the first one $\varepsilon \equiv 53 \bmod 81$, and at the second $z \equiv 55 \bmod 81$. Both $53^2 - 1$ and $55^2 - 1$ have valuation three. The two coordinates of each principal 3-unit sum to zero by reciprocity. Its logarithms are therefore divisible by nine in these cases, with exact valuation two. The generators above, including their index prime to three, show that the closed logarithm lattice is exactly $9Z^0$. Theorem 28.11 now gives $\widetilde{C}(D) \simeq \mathbb{Z}/9$.

When $2 \cdot 3^{h-1} \mid r$, the coefficient is trivial modulo 3^h. Apply Theorem 22.5 with $E = D$, $L = D(\mu_3)$, whose real subfield is D. The relative group acts trivially on the real class group and the coefficient. The resulting 3^h-torsion is $\mathrm{Hom}(\mathbb{Z}/9, \mathbb{Z}/3^h)$. For $h = 1$ this shows cyclicity of the finite strict group and the first lower bound. For $h = 2$ it gives the second lower bound. For $h = 3$ the 27-torsion has order nine, so the full group has no element of order 27 and is itself cyclic of order nine. Complex conjugation acts trivially on cohomology over the real field D, as it is represented by an element of its absolute Galois group. Finally $[E_x : D]$ is a power of two, so strict descent identifies the invariant summand at three with the one just computed. The complementary sign retains the even twists. Counting multiples gives both sums. □

28.13 Characteristic polynomials and capitulation in the real tower

Keep the interval and the prime $p > 2$ fixed. Use the ordinary unramified module M_p, the split quotient X_p, and $D_p = \ker(M_p \to X_p)$ of Theorem 22.8. The tame character and the field $E = E_x$ vary along this interval. Write $H = \mathrm{Gal}(E_*(\mu_{p^\infty})/E_*(\mu_p))$, with generator γ and cyclotomic value $a = \kappa_p(\gamma)$. As before, F_j denotes the layer of degree p^j above $(E_*(\mu_p))^+$.

Theorem 28.13 (The full order from the ordinary class module)**.** *The subgroup D_p is contained in the finite $\mathbb{Z}_p$-torsion subgroup C_p of M_p. Put $W_p = M_p/C_p$ and $C_p' = C_p/D_p$. For every E_x let Δ_x be the prime-to-p torsion subgroup of $G_x = \mathrm{Gal}(E_*(\mu_{p^\infty})/E_x)$. For a character τ of Δ_x with values in $\mathbb{Z}_p^\times$, write e_τ for its averaging idempotent and put*

$$P_{x,\tau}(Z) = \det(ZI - \gamma \mid e_\tau W_p) \in \mathbb{Z}_p[Z].$$

The determinant on a module of rank zero is one. For $r \geq 1$ put $\tau = \kappa_p^{-r}|_{\Delta_x}$ and $b = a^{-r}$. Then $P_{x,\tau}(b) \neq 0$ and the full complementary strict dual has order

$$|A_{p,x,r}| = p^{v_p(P_{x,\tau}(b))} |\ker(\gamma - b \mid e_\tau C_p')|. \tag{28.1}$$

The same polynomial computes the free contribution to the ordinary specialization $U_{p,x,r}$. In its order formula the finite group is $e_\tau C_p$. Both free lattices and finite groups in these formulas come from E_* for the whole interval.

Proof. Iwasawa's class module theorem identifies M_p with the inverse limit under norm of the p-parts of the ordinary ideal class groups of F_j. It is a finitely generated torsion module

over $\mathbb{Z}_p[[H]]$. The ground field F_0 is abelian over $\mathbb{Q}$ and F_∞/F_0 is its cyclotomic $\mathbb{Z}_p$-extension. Ferrero and Washington's theorem therefore gives $\mu = 0$. In the structure theorem over $\mathbb{Z}_p[[H]]$, all elementary factors then arise from powers of distinguished polynomials. Each such quotient is finite free over $\mathbb{Z}_p$ by polynomial division. The kernel and cokernel in the structure theorem are finite. It follows that M_p is finitely generated over $\mathbb{Z}_p$, C_p is finite, and W_p is finite free. [15, 16]

We show that $\omega_j = \gamma^{p^j} - 1$ is invertible on $W_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ for every j. Over F_j, the Galois group of the extension defining M_p is an extension of $H^{p^j} \simeq \mathbb{Z}_p$ by M_p. A lift of a generator splits this extension, since its closed procyclic subgroup maps onto $\mathbb{Z}_p$ with trivial kernel. The closed commutator group is $\omega_j M_p$. Consequently the kernel of the map from the abelianization to H^{p^j} is $M_p/\omega_j M_p$.

This abelianization is a quotient of the maximal abelian pro-p Galois group of F_j unramified outside p. That group has $\mathbb{Z}_p$-rank one. To verify the rank, use the ray class sequence with moduli supported at p and take its pro-p limit. The product of the local principal unit groups has rank $\sum_{v|p}[F_{j,v} : \mathbb{Q}_p] = [F_j : \mathbb{Q}]$. Its image has finite index, since the ideal class group is finite. Its kernel is the closure of the diagonal global units that are locally principal units. These form a subgroup of finite index in the global units. Brumer's theorem on Leopoldt's conjecture for abelian fields gives this closure rank $[F_j : \mathbb{Q}] - 1$, since F_j is totally real and abelian over $\mathbb{Q}$. [17] Thus $M_p/\omega_j M_p$ has rank zero after the rank-one quotient H^{p^j} is taken into account. On the rational vector space, ω_j is a surjective endomorphism and is therefore invertible.

Some H^{p^j} fixes every prime above p, since H acts continuously on the finite set of these primes. The corresponding Frobenius elements are then fixed, by the description in Theorem 22.8. Their images in W_p vanish because ω_j has zero kernel there. Thus $D_p \subset C_p$. In particular the torsion subgroup of $X_p = M_p/D_p$ is exactly C_p', and its quotient by torsion is W_p.

The index of H in G_x is prime to p. The factor over $E_*(\mu_p)/E_*$ divides $p-1$, and $[E_* : E_x]$ is a power of two. Since G_x is abelian it is the direct product $\Delta_x \times H$. Indeed, for $m = [G_x : H]$ and $g \in G_x$, the element $g^m \in H$ has a unique m-th root in H. Dividing g by this root gives a torsion lift of its coset. The intersection with H is trivial. The relations for Δ_x select exactly the image of

$$e_\tau = |\Delta_x|^{-1} \sum_{\delta \in \Delta_x} \tau(\delta)^{-1} \delta.$$

Indeed each relation kills this summand and $z - e_\tau z$ is a sum of relations. On the selected summand the relations for H amount to $\gamma - b$, since integral powers are dense and the image of this endomorphism is compact.

Apply these facts to $0 \to C_p' \to X_p \to W_p \to 0$. The cokernel on $e_\tau W_p$ is a quotient of the finite group $A_{p,x,r} = Q_{x,r}(X_p)$. Thus $\gamma - b$ on this free lattice has nonzero determinant, and has zero kernel. If a torsion element lies in the image of $\gamma - b$ on $e_\tau X_p$, its preimage maps to zero in the free lattice, so it already belongs to $e_\tau C_p'$. We obtain a short exact sequence of the three cokernels. Smith normal form gives the free cokernel order $p^{v_p(P_{x,\tau}(b))}$. On the finite group $e_\tau C_p'$ an endomorphism has kernel and cokernel of the same order. This proves (28.1). Applying the same argument to $0 \to C_p \to M_p \to W_p \to 0$ proves the assertion for $U_{p,x,r}$. □

Proposition 28.14 (The finite term as a capitulation kernel)**.** *Let $B_j = \widetilde{C}(F_j)$ be the degree-zero logarithmic class group. For all sufficiently large j, C_p' identifies, equivariantly for the field action, with the subgroup of B_j whose classes become zero under extension to some F_k, $k \geq j$. For each such j, one finite k realizes this entire kernel for all E_x and all twists.*

Proof. Use $B_j = X_p/\omega_j X_p$, as in Theorem 22.7. For $k > j$ write $\nu_{j,k} = \sum_{i=0}^{p^{k-j}-1} \gamma^{ip^j}$, so $\omega_k = \nu_{j,k}\omega_j$. Extension of a logarithmic class from F_j to F_k takes $z \bmod \omega_j X_p$ to $\nu_{j,k} z \bmod \omega_k X_p$. Indeed reciprocity sends extension on ideles to group transfer. Representatives given by the successive powers of a lift of γ^{p^j} conjugate z by the powers in this sum. This computation takes place in the group defining the split tower, hence passes to its degree-zero abelianized kernel at each level.

Both ω_k and ω_j are invertible on $W_p \otimes \mathbb{Q}_p$ by the preceding proof, so $\nu_{j,k}$ is injective on W_p. If a class represented by z dies at level k, then $\nu_{j,k}(z - \omega_j y) = 0$ for some $y \in X_p$. Projecting to W_p shows that the class of z has a representative in C_p'.

Choose j_0 so $H^{p^{j_0}}$ acts trivially on the finite group C_p', and choose $l \geq 0$ so $p^l C_p' = 0$. If $j \geq j_0$, then $\omega_j X_p \cap C_p' = \omega_j C_p' = 0$. The first equality follows from injectivity of ω_j on W_p. Thus C_p' injects into B_j. For $k \geq j + \max(1, l)$ the operator $\nu_{j,k}$ acts on C_p' as multiplication by p^{k-j}, which kills it. The two inclusions give the asserted equality. All maps commute with field automorphisms since the tower over $\mathbb{Q}$ is abelian. □

Formula (28.1) separates two arithmetic quantities in the remaining cohomology estimate. One needs a uniform bound for the valuations of the ordinary characteristic polynomials at the specified positive twists together with the finite kernels on the capitulating classes. The proposition supplies a finite level for each fixed prime and interval. It gives no uniform bound on that level as the prime and interval vary.

28.14 A determinant for full strict orders and the first class norm

An order bound from the first two ordinary class groups can be made for all but an explicitly bounded number of twists. We use a determinant which includes the finite subgroup of the cyclotomic module. All valuations in this subsection give p value one. For a finite $\mathbb{Z}_p$-module B, write $\ell(B) = \log |B| / \log p$.

Lemma 28.15 (Simultaneous specialization of a finite presentation)**.** *Let M be a finitely generated $\mathbb{Z}_p$-module, G an endomorphism, and S a finite set of algebraic p-adic integers. Take a finite extension $K/\mathbb{Q}_p$ containing S, with ring of integers O and ramification index e_K. Suppose that for every $z \in S$ the quotient $B_z = (M \otimes O)/(G - z)(M \otimes O)$ is finite. There is a monic polynomial P over the integers of a finite unramified extension of K such that, simultaneously,*

$$v_p(P(z)) = \operatorname{length}_O(B_z)/e_K \qquad (z \in S).$$

One may take $\deg P = \dim_{\mathbf{F}_p}(M/pM)$.

Proof. Choose a minimal presentation of M over $\mathbb{Z}_p$ in Smith form, with n generators and relation matrix Q. Its columns are the nonzero powers of p times the basis vectors belonging to the finite summands. Lift G to an n by n matrix A on the generators. At z the presentation matrix is $[\, zI - A, Q \,]$. Since its cokernel is finite, the minimum valuation of its maximal minors is the number on the right, by Smith normal form over O. For $n = 0$ take $P = 1$.

Let Z be a matrix of independent variables with as many rows as Q has columns and with n columns. In $\det(zI - A + QZ)$, expand by multilinearity in its columns. Each coefficient is zero or a signed maximal minor of the presentation matrix. Conversely, choose any n columns of that matrix. Match the selected columns of Q to the omitted positions of $zI - A$. The monomial made from these entries of Z specifies precisely those replacements. Its coefficient is the chosen minor up to sign. Thus the minimum valuation of the coefficients is the required minimum. Divide the polynomial at each z by a scalar of that minimum valuation and reduce it in the

residue field. The product of the resulting polynomials is nonzero. Over the algebraic closure of the residue field it has a point where it is nonzero, since that field is infinite. The finitely many coordinates lie in a finite extension of the residue field. Lift them to a matrix Z_0 in the corresponding unramified extension of O. Taking $P(X) = \det(XI - A + QZ_0)$ gives all the required equalities. Extension of the residue field has preserved the normalized valuations. □

Fix an interval of Section 6.6, its largest field E_*, an odd prime p, and $a = \kappa_p(\gamma)$ as in Theorem 22.7. Set $d = v_p(a-1)$, $s_r = d + v_p(r)$. Take an integer $t_* > 1$ above all the weight cutoffs on this interval. Keep the tame group Δ_0, the idempotent e removing the invariants for D', and the idempotent e_τ of Theorem 22.4. Write $X = X_p$ for the split class module of Theorem 28.13. For a character τ put

$$M = e_\tau e X, \quad c_\tau = \ell(C_{0,\tau}), \quad k_\tau = \ell \ker(C_{1,\tau} \longrightarrow C_{0,\tau}), \quad H = d + \lfloor \log(t_*)/\log p \rfloor.$$

Here the map between the ordinary class groups is norm. Only weights with $\kappa_p^{-r}|_{\Delta_0} = \tau$ are used in this component.

Theorem 28.16 (Two independent bounds for exceptional twists)**.** *For each τ there are two sets D_τ^0, D_τ^1 of these weights in $1 \le r < t_*$, of cardinalities at most $\lfloor c_\tau/d \rfloor$ and k_τ respectively. The same sets work for every E_x of the interval. If $B_r = eA_{p,x,r}$ is the indicated summand of the full complementary strict dual, then*

$$\begin{aligned} r \notin D_\tau^0 \quad &\Longrightarrow \quad \ell(B_r) \le H c_\tau/d, \\ r \notin D_\tau^1 \quad &\Longrightarrow \quad \ell(p^{s_r} B_r) \le H k_\tau. \end{aligned}$$

In particular the second bound counts the full remaining length above the base precision. It includes the finite classes that capitulate.

Proof. Put $b_r = a^{-r}$. The strict dual over E_* in this component is $M/(\gamma - b_r)M$, by Theorem 28.13 and its proof. Over E_x the larger group of field automorphisms imposes further relations, so its component is a quotient. All positive-twist quotients over E_* are finite. Moreover $M/(\gamma-1)M = C_{0,\tau}$. Put $U = (\gamma-1)M$ and $N_p(Y) = 1 + Y + \cdots + Y^{p-1}$. The kernel of the first class norm is $U/N_p(\gamma)U$, since $\gamma^p - 1 = N_p(\gamma)(\gamma - 1)$, by Theorem 22.4. The image of U in B_r equals $(b_r - 1)B_r = p^{s_r}B_r$. The modules M, U are finitely generated over $\mathbb{Z}_p$ by Theorem 28.13. On their rational spans $\gamma - b_r$ is injective, first on M by finiteness and then on its stable subspace spanned by U.

Apply Lemma 28.15 to M with the points $1, b_r$. The roots of the monic polynomial are integral. Their distances to 1, measured by valuation and summed with multiplicity, total c_τ. A root α with $v_p(\alpha - 1) < d$ contributes precisely that same valuation at every b_r. There are at most $\lfloor c_\tau/d \rfloor$ other roots. For each of these choose a weight r_0 in the progression maximizing $v_p(b_{r_0} - \alpha)$, provided the progression is nonempty. At every other weight the ultrametric inequality and the binomial calculation of Theorem 22.7 give

$$v_p(b_r - \alpha) \le v_p(b_r - b_{r_0}) = d + v_p(r - r_0) \le H.$$

Use the chosen weights as D_τ^0. Since $H \ge d$, the sum over all roots at a remaining weight is at most Hc_τ/d.

For U take as reference point a primitive p-th root ζ and again include all the b_r. Its coefficient ring $O = \mathbb{Z}_p[\zeta]$ has ramification index $p-1$ and residue field $\mathbf{F}_p$. Evaluating Y at γ identifies

$$(U \otimes O)/(\gamma - \zeta)(U \otimes O) \simeq U/N_p(\gamma)U.$$

Indeed $O = \mathbb{Z}_p[Y]/N_p(Y)$, and the further relation identifies multiplication by Y with γ on generators of U. Thus the reference valuation in the lemma is $k_\tau/(p-1)$. At $b_r \in \mathbb{Z}_p$ the normalized valuation equals the original $\mathbb{Z}_p$-length, by flat scalar extension. Now $v_p(b_r - \zeta) = 1/(p-1)$ for every positive r. At most k_τ roots α satisfy $v_p(\alpha - \zeta) \geq 1/(p-1)$. For each such root select a closest b_{r_0} as above to form D^1_τ. All other roots contribute their reference valuation at every b_r. If that latter sum is S, the number selected, with multiplicity, is at most $k_\tau - (p-1)S$. At an unselected weight the valuation is at most $S + H(k_\tau - (p-1)S) \leq Hk_\tau$. Passing to the image of U proves the second assertion. □

Corollary 28.17 (A class norm bound on the common intervals)**.** *Let $t = \lfloor x^{401} \rfloor$, $Y = x^{-3}\exp(x^\varepsilon/4)$, $Z = x^{-3}\exp(x^\varepsilon/6)$, with $0 < \varepsilon < 1/52$. For $p \leq Z$ retain in $B_r = eA_{p,x,r}$ only terms with $r \in D^0_\tau \cap D^1_\tau$. For $Z < p \leq Y$ retain terms with $r \in D^0_\tau$. Summed over these odd primes and $1 \leq r < t$, the logarithmic orders of all the discarded B_r are $O_{\psi,\varepsilon}(x^{-2}\exp(x^\varepsilon/2))$. At $p \leq Z$ the exceptional count for each component is at most $\min(\lfloor c_\tau/d \rfloor, k_\tau)$. Both ordinary class groups and both selections use the same largest field throughout an interval.*

Proof. For $r \notin D^0_\tau$ use the first bound of the theorem. For $p \leq Z$ and $r \notin D^1_\tau$, the base term $B_r/p^{s_r}B_r$ is a quotient of $C_{0,\tau}$ by Theorem 22.4. Thus $c_\tau + Hk_\tau$ bounds the full length in this case. For $n_* = [E_* : \mathbb{Q}]$ there are at most $1 + tn_*/(p-1)$ occurrences of each τ. Orthogonal tame idempotents give $\sum_\tau c_\tau \log p \leq \log|\mathrm{Cl}(F_0)|$ and $\sum_\tau k_\tau \log p \leq \log|\mathrm{Cl}(F_1)|$. The conductors and the Minkowski estimate in Theorem 9.16 bound these class number logarithms by $O(n_* p^{j+1}\log(2N_* n_* p^{j+1}))$ for $j = 0, 1$, where N_* is the modulus for E_*. One may take $t_* = 2 + \lceil V^{602} \rceil$, so $H \ll_\psi \log(2x)$ since $p^{d-1} \leq n_*$. For $p \leq Y$ the conductor logarithm is $O_{\psi,\varepsilon}(x^\varepsilon)$ and $n_* \ll_\psi x^{3+12\varepsilon}$. Bounding the sums over primes by sums over integers now gives a constant times

$$n_* x^\varepsilon \log(2x)(Y^2 + tn_* Y + Z^3 + tn_* Z^2).$$

The Y^2 term is $O(x^{-3+13\varepsilon}\log(2x)\exp(x^\varepsilon/2))$. The Z^3 term has $x^{-6+13\varepsilon}$ in its place. The remaining powers of x multiply at most $\exp(x^\varepsilon/3)$. These estimates prove the stated bound. They concern the component cut out by e. □

Proposition 28.18 (One exceptional order with fixed norm groups)**.** *In the category of finitely generated cyclotomic modules, the orders of the norm groups at every layer, even with their transition maps on underlying groups, give no uniform bound on a single exceptional positive-twist order.*

Proof. Fix $r_0 \geq 1$ and $a \in 1 + p\mathbb{Z}_p$ of infinite order. On $M = \mathbb{Z}_p$ let a topological generator γ act by $a^{p^L - r_0}$, where $p^L > r_0$ and $L > v_p(r_0)$. This defines a continuous action of $\mathbb{Z}_p$. For every $j \geq 0$, the ideal $(\gamma^{p^j} - 1)M$ is $p^{d + v_p(r_0) + j}M$, independent of L. The norm quotients are the same cyclic groups with the same reduction maps. On the other hand $\gamma - a^{-r_0} = a^{-r_0}(a^{p^L} - 1)$ has valuation $d + L$. All positive-twist quotients are finite, since $p^L - r_0 > 0$. Thus even when every first difference of norm lengths equals one, the length at r_0 can grow arbitrarily. This example concerns the module argument. Deciding which such orders the arithmetic towers realize requires information about their field actions. □

28.15 A decomposition group that detects every strict class

Let ℓ be an odd prime and $b \neq \ell$ a prime congruent to one modulo ℓ. Let $\mathcal{F}$ be the maximal pro-ℓ extension of $\mathbb{Q}$ unramified away from ℓ, b, and put $\mathcal{G} = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$. The extensions considered here may ramify at both primes. We use two elementary tests,

$$\ell^{(b-1)/\ell} \not\equiv 1 \pmod{b}, \qquad b^{\ell-1} \not\equiv 1 \pmod{\ell^2}. \tag{28.2}$$

The second test is equivalent to $b \not\equiv 1 \bmod \ell^2$ under our assumption on b. The two tests concern different places.

Lemma 28.19 (The maximal elementary abelian quotient)**.** *The maximal elementary abelian quotient of $\mathcal{G}$ has dimension two over $\mathbf{F}_\ell$. A decomposition group at ℓ is all of $\mathcal{G}$ if and only if the first test in (28.2) holds. A decomposition group at b is all of $\mathcal{G}$ if and only if the second test holds.*

Proof. By Kronecker–Weber, every cyclic extension of $\mathbb{Q}$ of degree ℓ unramified away from these primes has character factoring through the unit groups modulo a power of ℓ and a power of b. At ℓ the principal units are topologically cyclic and give one quotient of order ℓ, already at modulus ℓ^2. At b the principal units are pro-b, and $\mathbf{F}_b^\times$ is cyclic of order divisible by ℓ. This gives one more quotient, already at modulus b. The two degree-ℓ fields so obtained have relatively prime conductors, and hence are linearly disjoint. For example, their intersection would be an abelian extension of $\mathbb{Q}$ unramified at every finite prime and of odd degree, so has degree one. Their compositum is the maximal elementary abelian subextension. [4, Chapters V and VI]

In its Galois group inertia at ℓ spans the first factor. The image of a decomposition group there in the second factor is generated by the class of ℓ in $\mathbf{F}_b^\times/(\mathbf{F}_b^\times)^\ell$. This class is nontrivial precisely in the first test. At b inertia spans the second factor, and Frobenius on the first is the image of b in the degree-ℓ quotient of $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. It is nontrivial precisely in the second test. For $b = 1 + \ell u$, the binomial expansion of $b^{\ell-1}$ modulo ℓ^2 proves the equivalence stated above.

A proper closed subgroup of a pro-ℓ group has proper image in some finite quotient. Indeed a point outside the subgroup has a coset neighborhood disjoint from it. A proper subgroup of the resulting finite ℓ-group lies in a maximal subgroup, which is normal of index ℓ. Pulling back that subgroup shows that the original closed subgroup fails to surject onto some cyclic quotient of order ℓ. Decomposition groups are closed. Thus surjectivity onto the two-dimensional elementary abelian quotient is equivalent to equality with $\mathcal{G}$. □

Theorem 28.20 (Detection over every finite layer)**.** *Suppose one of the tests in (28.2) holds, and let v be its corresponding place. Let B be any finite intermediate field of $\mathcal{F}/\mathbb{Q}$, and let w be its place over v. It is unique. Let O be the integers in a finite extension $J/\mathbb{Q}_\ell$ with uniformizer π. Suppose $\vartheta : G_B \to O^\times$ is continuous, trivial modulo π, and unramified away from the places over ℓ, b. On degree-one classes with coefficients $(J/O)(\vartheta)$ unramified away from these same places, localization at w is injective.*

Proof. By Lemma 28.19 the image of a local decomposition group at v in $\mathcal{G}$ is the whole group. It acts transitively on the embeddings of B into $\mathcal{F}$ and hence there is one place above v. Its subgroup fixing the chosen embedding of B surjects onto $\mathrm{Gal}(\mathcal{F}/B)$. Equivalently the image of G_{B_w} is that entire subgroup.

Let z represent a class in the kernel of localization. For some $y \in J/O$ one has $z(h) = (\vartheta(h) - 1)y$ on G_{B_w}. The image of z is finite by continuity, compactness of G_B and discreteness of J/O. Choose m so that y and every value of z lie in $A_m = (J/O)[\pi^m]$. The map

$$g \longmapsto (z(g),\ \vartheta(g) \bmod \pi^m)$$

is a homomorphism to the semidirect product of A_m with the image of $\vartheta \bmod \pi^m$. This is a finite ℓ-group, since the character takes values in principal units modulo π^m. Away from ℓ, b inertia acts trivially and a coboundary on inertia is the zero cocycle. Thus the finite Galois extension of B cut out by this map is unramified there.

This finite extension is contained in $\mathcal{F}$ even if $B/\mathbb{Q}$ is not Galois. Indeed a finite Galois ℓ-extension inside $\mathcal{F}$ contains the normal closure of B. Base change all conjugates of the finite extension just cut out by the homomorphism to that Galois field. Each compositum with it is Galois of ℓ-power degree over it. Their joint compositum is Galois of ℓ-power degree over $\mathbb{Q}$ and is unramified at every prime outside ℓ, b. It lies in $\mathcal{F}$. Consequently every value of the displayed homomorphism occurs already on G_{B_w}. The identity $z(g) = (\vartheta(g) - 1)y$ depends only on that value, by the choice of m. It holds on all of G_B, proving that the class is zero. □

Corollary 28.21 (Full vanishing on the original period fields)**.** *Write* $\mathrm{Gal}(E_x/\mathbb{Q}) = P \times H$ *with* P *its* ℓ*-Sylow group,* H *of order prime to* ℓ*, and let* $B = E_x^H$*. Suppose* B *is unramified away from* ℓ, b *and at least one of the two tests in* (28.2) *holds. For every character* β *of* H*, extended trivially on* P*, and every positive* r *with* $\bar{\beta}^{-1}\bar{\kappa}_\ell^{-r} = 1$ *on* G_B*, the entire* β*-component of* $\mathcal{S}_{\ell,r}(E_x)$ *over* $\mathbb{Z}_\ell[\beta]$ *vanishes. This holds at every* x *of the interval and at every exponent. If* B *is unramified away from* ℓ *alone, the same vanishing holds with no test at* b*.*

For a scalar character α *of* E_x *with* $\bar{\alpha}^{-1}\bar{\kappa}_\ell^{-r} = 1$ *on* $G_{\mathbb{Q}}$ *and conductor supported on* ℓ, b*, the stronger local group* $S^{N_*}(\alpha, r)$ *of Theorem 22.17 also vanishes under either test. Under the first test already* $S(\alpha, r) = 0$*. Under the second test* $S(\alpha, r)$ *injects into the unramified local group at* b *of Lemma 22.16.*

Proof. Restriction induces an isomorphism between the β-component and the strict group over B for $\vartheta = \beta^{-1}\kappa_\ell^{-r}$ with divisible coefficients. Indeed restriction to E_x gives the invariants of the twisted module by inflation–restriction, since $|H|$ is a unit. Untwisting on G_{E_x} selects the indicated character. At places above ℓ and on inertia elsewhere the corresponding indices are prime to ℓ, so restriction also detects the local conditions. This is the integral descent of Lemma 24.8. Since $G_{\mathbb{Q}}/G_B$ has ℓ-power order and the residual character has order prime to ℓ, triviality on G_B implies triviality on $G_{\mathbb{Q}}$. The prime-to-ℓ character β is therefore the Teichmüller lift of $\bar{\kappa}_\ell^{-r}$, and is unramified away from ℓ.

The field B is an abelian ℓ-extension in $\mathcal{F}$. Under the first test apply Theorem 28.20 at ℓ, where a strict class is zero. Under the second apply it at b. There the coefficient is unramified, and arithmetic Frobenius acts by a root of unity times $(Nw)^{-r}$. This scalar differs from one as $r > 0$. Its difference from one acts surjectively on the divisible coefficient. Thus the unramified local cohomology is zero, also over a ramified field B_w. In both cases injectivity proves the asserted full vanishing. The relative degree of E_x/K_ψ is a power of two, so B is precisely the maximal ℓ-subfield of the fixed K_ψ. In particular the ramification condition on B is independent of x. If B is unramified away from ℓ alone, use the maximal pro-ℓ extension unramified away from ℓ alone. Its elementary abelian quotient is the first cyclic factor in Lemma 28.19. Inertia at ℓ surjects onto it. The same closed-subgroup and localization proofs apply.

For the scalar assertion use Theorem 28.20 with base $\mathbb{Q}$ and $\vartheta = \alpha^{-1}\kappa_\ell^{-r}$. The first test gives injectivity at ℓ. Under the second, restriction at b is injective and its image for $S(\alpha, r)$ is unramified. If α is ramified at b then $b \mid N_*$ and S^{N_*} imposes zero there. If α is unramified there, the unramified local group already vanishes. □

Proposition 28.22 (Split coefficient primes in the cubic example and beyond)**.** *For each odd prime* ℓ*, the primes* $b \equiv 1 \bmod \ell$ *for which* ℓ *splits completely in the degree-*ℓ *subfield of* $\mathbb{Q}(\zeta_b)$ *and* $b \not\equiv 1 \bmod \ell^2$ *have natural density* $1/\ell^2$ *among rational primes. In particular take* $\ell = 3$*,* $b = 61$*, and a primitive cubic character* ψ *of conductor* 61*. On every one of its period fields the full* $\mathrm{Gal}(E_x/K_\psi)$*-invariant complementary group at three is zero for every positive twist.*

Proof. For $b \equiv 1 \bmod \ell$, complete splitting of ℓ in the specified degree-ℓ field means that ℓ is an ℓ-th power modulo b. Away from ℓ this and the congruence $b \equiv 1 \bmod \ell$ mean that b splits

completely in $D = \mathbb{Q}(\mu_\ell, \sqrt[\ell]{\ell})$, the splitting field of $X^\ell - \ell$. Over $L = \mathbb{Q}(\mu_\ell)$ the fields D and $C = \mathbb{Q}(\mu_{\ell^2})$ are distinct cyclic extensions of degree ℓ. In the Kummer group $L^\times/L^{\times\ell}$ their defining classes are ℓ and ζ_ℓ. At the unique prime above ℓ, the first class has valuation $\ell - 1$ modulo ℓ, and the second has valuation zero. The second class is nonzero because $[C : L] = \ell$. They span distinct lines, hence $D \cap C = L$. The group of $DC/\mathbb{Q}$ has order $\ell^2(\ell-1)$. Exactly $\ell-1$ of its elements restrict to the identity on D and nontrivially to C. This is a conjugacy-stable set and Chebotarev gives the stated density. [4, Chapter VI]

For $b = 61$ one has $3^5 \equiv -1 \bmod 61$, whence $3^{20} \equiv 1 \bmod 61$, while $61 \equiv 7 \bmod 9$. Thus 3 splits in K_ψ and the test at 61 holds. For even r take $\beta = 1$ in Corollary 28.21. For odd r the complementary sign is minus. It is zero on the invariants from K_ψ, since this odd-degree Galois field is totally real, so complex conjugation is the identity in its Galois group over $\mathbb{Q}$. The descent just proved identifies these invariants with the asserted subgroup on E_x. □

The two local tests control the indicated components, including twists for which the residue character is trivial and a uniform bound just from the orders of successive class groups is unavailable. The other character components and the comparison of the prescribed integral theta periods remain to be bounded in Section 6.6.

29 References

[1] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997. Chapter 6, Stickelberger's theorem.

[2] A. V. Sutherland, *The Kronecker–Weber theorem*, MIT 18.785, Lecture 20. Lecture notes.

[3] R. Sharifi, *Group and Galois Cohomology*, Section 2.5, Lemma 2.5.8. Kummer isomorphism.

[4] J. S. Milne, *Class Field Theory*. Local and global Artin reciprocity and the correspondence with idele class quotients.

[5] O. Ramaré, *Approximate formulae for $L(1,\chi)$*, Acta Arith. **100** (2001), 245–266. Corollary 1, p. 248.

[6] R. Osburn, *Vanishing of eigenspaces and cyclotomic fields*. Theorem 1.1, the rational cyclotomic case.

[7] T. Morisawa and R. Okazaki, *Height and Weber's Class Number Problem*, J. Théor. Nombres Bordeaux **28** (2016), 811–828. Corollary B.

[8] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006. Part I, Sections 2 and 4.

[9] C. A. Weibel, *The K-book. An introduction to algebraic K-theory*, Graduate Studies in Mathematics 145, American Mathematical Society, 2013. Chapter VI, Section 8.

[10] J. Voight, *The Gauss higher relative class number problem*. Proposition 1.3 and its odd-prime form.

[11] T. Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan **38** (1986), 95–102. Theorem 2, pp. 95–96, and the table on p. 99.

[12] 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.

[13] J. S. Milne, *Arithmetic Duality Theorems*, 2nd ed., 2006, Chapters I and II. Book.

[14] C. Greither and C. D. Popescu, *An equivariant main conjecture in Iwasawa theory and applications*, J. Algebraic Geom. **24** (2015), 629–692. Authors' paper.

[15] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[16] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395. Original paper.

[17] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124. Original paper.