EXCEPTIONAL TWISTS IN CYCLOTOMIC TOWERS

Prerequisites. Chapter 30, *Tate–Shafarevich groups of Tate twists*: the modules $W_e = \mathbb{Q}_\ell/\mathbb{Z}_\ell(-e)$, the groups $\mathrm{Sha}_\ell(F,e)$ and their lengths $h_{\ell,e}(F)$, Problems 30.1.1 and 30.2.1, and Theorem 30.1.2. Iwasawa's theory of $\mathbb{Z}_\ell$-extensions and $\Lambda = \mathbb{Z}_\ell[[T]]$-modules [Wa, Ch. 13]; continuous cohomology and the duality theorems of Poitou and Tate [NSW, Ch. VII–VIII]. In this chapter ℓ is any prime, 2 included. For a number field F, $G_{F,\ell}$ is the Galois group of the largest extension of F unramified outside ℓ and ∞, and $\mathrm{Sha}_\ell(F,e)$ is the group of classes in $H^1(G_{F,\ell}, W_e)$ that vanish on the decomposition groups at all places above ℓ. We write $\mu'_\ell = \mu_\ell$ if ℓ is odd and $\mu'_2 = \mu_4$.

54.1. Layers

In Alpöge's argument the twist e runs up to a power of the scale x, and the field changes with x. Along which fields do the lengths $h_{\ell,e}$ stay small uniformly in e, and how does this fail? Iwasawa's answer: along a cyclotomic tower they grow linearly with the layer, except at twists e that are ℓ-adically close to finitely many points.

Let L_0 be a number field inside a fixed algebraic closure of $\mathbb{Q}$. A *layer of degree* ℓ^m over L_0 is a field $L_0(\zeta_{\ell^k})$, $k \geq 0$, with $[L_0(\zeta_{\ell^k}) : L_0] = \ell^m$.

Problem 54.1.1. Suppose $\mu'_\ell \subset L_0$. Then $L_\infty := L_0(\mu_{\ell^\infty})$ is a $\mathbb{Z}_\ell$-extension of L_0, and for every $m \geq 0$ there is exactly one layer L_m of degree ℓ^m over L_0: the fixed field of $\mathrm{Gal}(L_\infty/L_0)^{\ell^m}$.

Problem 54.1.2. Over $L_0 = \mathbb{Q}$ and $\ell = 2$ the layers are the fields $\mathbb{Q}(\zeta_{2^k})$. The layer of degree 2 is $\mathbb{Q}(i)$, which does not lie in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, the union of the real fields $\mathbb{Q}(\zeta_{2^k} + \zeta_{2^k}^{-1})$.

This is why μ_4 is required when $\ell = 2$. The discriminants of the layers are controlled by the conductor.

Problem 54.1.3. If a number field L contains a primitive ℓ^k-th root of unity, then $\ell^k \leq 2[L:\mathbb{Q}]$.

Problem 54.1.4. If $L \subseteq \mathbb{Q}(\zeta_N)$, then $|\Delta_L| \leq N^{[L:\mathbb{Q}]}$.

Problem 54.1.5. Let $L_0 \subseteq \mathbb{Q}(\zeta_{N_0 P})$ with $[L_0:\mathbb{Q}] \leq n_1$, and let L be a layer of degree ℓ^j over L_0. Then $[L:\mathbb{Q}] \leq n_1 \ell^j$ and $\log(2|\Delta_L|) \leq C(1 + \log P)$, with C depending only on ℓ, j, n_1 and N_0.

In the application $P = qd$ is the product of the two auxiliary primes, and $\log P$ is at most a small power of the scale.

Date: November 26, 2026.

54.2. Where the lengths grow

Let ℓ be odd, let $\kappa \in 1+\ell\mathbb{Z}_\ell$ with $v_\ell(\kappa-1)=1$, and for $y\in\mathbb{Z}_\ell$ put $\kappa^y = \exp(y\log\kappa)$. In a $\mathbb{Z}_\ell$-extension a generator γ of the Galois group acts on $\mathbb{Z}_\ell(-e)$ by such a power of κ, and Iwasawa's theory compares the groups at the m-th layer with the coinvariants of γ^{ℓ^m} on a module attached to the whole tower [Wa, Ch. 13]. Here is a model.

Problem 54.2.1. For $y\in\mathbb{Z}_\ell$, $v_\ell(\kappa^y-1)=1+v_\ell(y)$.

Problem 54.2.2. Let $s\in\mathbb{Z}_\ell$, $e\in\mathbb{Z}$, $m\geq 0$, and let γ act on $X=\mathbb{Z}_\ell$ by κ^{s-e}. Then $\operatorname{len}_{\mathbb{Z}_\ell} X/(\gamma^{\ell^m}-1)X = m+1+v_\ell(s-e)$, infinite if $s=e$.

Problem 54.2.3. Let γ act on $X=\mathbb{Z}_\ell^r$ by an upper triangular matrix with diagonal entries $\kappa^{s_1-e},\dots,\kappa^{s_r-e}$. If $v_\ell(s_i-e)\leq B$ for all i, then $\operatorname{len}_{\mathbb{Z}_\ell} X/(\gamma^{\ell^m}-1)X \leq r(m+1+B)$.

So the length is linear in the layer m and in B, and blows up only for twists e near one of the *centres* s_i. Near how many twists?

Problem 54.2.4. Let s lie in a field containing $\mathbb{Q}_\ell$ with an absolute value $|\cdot|_\ell$ extending that of $\mathbb{Q}_\ell$, let $Z\geq 1$, and $B=\lfloor\log_\ell Z\rfloor$. At most one integer $1\leq e\leq Z$ satisfies $|s-e|_\ell<\ell^{-B}$.

Problem 54.2.5. For $\ell=5$, $s=-1/3\in\mathbb{Z}_5$ and $Z=10^4$ one has $B=5$; the only $e\leq Z$ with $v_5(s-e)>5$ is $e=5208$, with $v_5(s-e)=6$, while $v_5(s-2083)=5$.

Exceptional twists are not an artefact of the model. By Theorem 30.1.2, for odd e with $(\ell-1)\nmid(e+1)$,

$$h_{\ell,e}(\mathbb{Q}) = v_\ell\big(\operatorname{num}(B_{e+1}/(e+1))\big).$$

Problem 54.2.6. Let $1\leq e<49284$ be odd with $e\equiv 31 \pmod{36}$. Then $h_{37,e}(\mathbb{Q})=1$ unless $e\equiv 283 \pmod{1332}$, and then $h_{37,e}(\mathbb{Q})\geq 2$. The only such e with $h_{37,e}(\mathbb{Q})\geq 3$ is $e=37579$, where $h_{37,e}(\mathbb{Q})=3$.

Problem 54.2.7. For every $e\geq 1$, $h_{37,e}(\mathbb{Q}(\zeta_{37}))\geq h_{37,e}(\mathbb{Q})$. Hence over $L_0=\mathbb{Q}(\zeta_{37})$, which contains μ_{37}, the lengths at the bottom layer are at least 3 at $e=37579$.

54.3. Ferrero–Washington and the tower bound

What makes the lengths along a tower linear rather than exponential in m is the vanishing of Iwasawa's μ-invariant. Let $\Lambda=\mathbb{Z}_\ell[[T]]$ and $\omega_m=(1+T)^{\ell^m}-1$.

Problem 54.3.1. Let X be a finitely generated Λ-module with $\dim_{\mathbb{F}_\ell} X/(\ell,\omega_m)X\leq r$ for all m. Then X is generated by r elements as a $\mathbb{Z}_\ell$-module.

For the class groups of the layers, Iwasawa's theory turns a bound for their ℓ-ranks into such a bound for the inverse limit of their ℓ-parts [Wa, Ch. 13]. The bound for the ranks is the theorem of Ferrero and Washington, in the following form.

Theorem 54.3.1 (Ferrero–Washington)**.** *Let K be an abelian number field with $\mu_\ell'\subset K$. There is r such that $|\mathrm{Cl}(K')/\mathrm{Cl}(K')^\ell|\leq\ell^r$ for every layer K' over K.*

Status: Ferrero and Washington proved $\mu = 0$ for abelian fields [FW]; Sinnott gave another proof [Si]; the bounded-rank form follows by Iwasawa's theory [Wa, Ch. 13]. The Lean formalization [Lean] proves Theorem 54.3.1 itself. The names of its steps (Stickelberger annihilation, an ℓ-adic independence lemma of Sinnott, Kummer reflection) indicate Sinnott's route; we have not read that proof.

The formalization deduces from this a bound along the tower. Put $j_0 = \lfloor \log_\ell R \rfloor + 3$.

Lemma 54.3.2 (tower bound)**.** *Let L_0 be totally imaginary with $\mu'_\ell \subset L_0$, with layers L_m, and suppose that a certain Iwasawa module of L_∞ is generated by $R \geq 1$ elements over $\mathbb{Z}_\ell$.*

(a) *There are $c_0 \geq 0$ with $\mu_{\ell^{c_0}} \subset L_0$, $r \leq R$, and $s_1, \dots, s_r$ in a field containing $\mathbb{Q}_\ell$, such that for all $e \geq 1$, $m \geq 0$ and integers $B \geq 0$ with $|s_i - e|_\ell \geq \ell^{-B}$ for every i, $h_{\ell,e}(L_m) \leq r(\max(m, j_0) + c_0 + B)$.*

(b) *For all $e \geq 1$ and $m \geq 0$, $h_{\ell,e}(L_m) \leq \operatorname{len}_{\mathbb{Z}_\ell} H^2(G_{L_{j_0},\ell}, \mathbb{Z}_\ell(e+1)) + R\max(m - j_0, 0)$.*

Status: proved in the Lean formalization, from the generator bound, Poitou–Tate duality and local Tate duality. For abelian L_0 the generator bound is deduced there from Theorem 54.3.1. We have not identified the Iwasawa module, and we have not read how the centres s_i arise; the formalization does not say that they are the zeros of a characteristic power series, as Problem 54.2.3 suggests. Part (a) is stated in this form in [Zh, §5.5].

Part (b) compares Sha with H^2. Let L be totally imaginary, or ℓ odd, and $e \geq 1$. By Poitou–Tate duality and local duality [NSW, Ch. VII, §2; Ch. VIII, §6], when all lengths are finite,

$$\operatorname{len} H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1)) + \operatorname{len} H^0(G_{L,\ell}, W_e) = h_{\ell,e}(L) + \sum_{v \mid \ell} \operatorname{len} H^0(G_v, W_e). \quad (1)$$

For $e \geq 1$ the group $H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1))$ is finite [So79], and $\mathrm{Sha}_\ell(L, e)$ is dual to a subgroup of it, so all lengths in (1) are finite.

Problem 54.3.2. Let ℓ be odd, $\mu_\ell \subset L$, and $\ell^c = |\mu_{\ell^\infty}(L)|$. For $e \neq 0$, $\operatorname{len} H^0(G_{L,\ell}, W_e) = c + v_\ell(e)$.

Problem 54.3.3. In Problem 54.3.2, for $e \geq 1$, $h_{\ell,e}(L) \leq \operatorname{len} H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1)) + c + v_\ell(e)$.

54.4. Second cohomology and the exceptional twists

At the exceptional twists only a bound for the whole group H^2 is available.

Theorem 54.4.1 (bound for H^2)**.** *There is an absolute constant C_H such that for every prime ℓ, every totally imaginary number field L with $\mu'_\ell \subset L$, and every $e \geq 1$, the group $H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1))$ is finite and*

$$\log\bigl|H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1))\bigr| \leq \exp\bigl((2e[L:\mathbb{Q}])^{C_H} \log(2|\Delta_L|)\bigr).$$

Status: finiteness is due to Soulé [So79]. Soulé also bounds these groups through the torsion in the homology of $\mathrm{GL}_n(\mathcal{O}_L)$ [So03], but only for ℓ large compared with e and $[L:\mathbb{Q}]$; we know no published estimate covering every ℓ, as noted in [Rub, §III.9]. The Lean formalization proves Theorem 54.4.1, by way of a rank bound for

the homology of $\mathrm{GL}_n(\mathcal{O}_L)$ of Borel's type; we have not read that proof. The bound is stated in [Zh, §5.5].

The bound is doubly exponential in e. It is useful only for small twists.

Problem 54.4.1. Let ℓ and L be as in Theorem 54.4.1, $x \ge 1$, $\varepsilon > 0$, $[L:\mathbb{Q}] \le n_0$, $\log(2|\Delta_L|) \le c_1 x^{\varepsilon/4}$, and $1 \le e \le x^{\varepsilon/(2C_H)}$. Then $\operatorname{len} H^2(G_{L,\ell}, \mathbb{Z}_\ell(e+1)) \le 2\exp(Cx^{3\varepsilon/4})$ with $C = (2n_0)^{C_H} c_1$.

Problem 54.4.2. Let $C_H \ge 1$, $b = \exp(x^\varepsilon)$ with $0 < \varepsilon < 1$, and $e \ge x$. Then the right side of Theorem 54.4.1 exceeds $\sqrt{b}$ for every $x \ge 1$, whatever L.

Compare Problem 30.3.2: the target in the argument is a bound by $\sqrt{b}$ for a sum of $\log \ell$ times lengths. Problem 54.2.4, Lemma 54.3.2 and Theorem 54.4.1 give the following.

Theorem 54.4.2 (twists along a tower)**.** *Let L_0 and R be as in Lemma 54.3.2, and $n = [L_{j_0} : \mathbb{Q}]$. For every $Z \ge 1$ there is a set $\mathcal{E}$ of at most R integers in $[1, Z]$ such that for every $m \ge 0$ and $1 \le e \le Z$,*

$$h_{\ell,e}(L_m) \le \begin{cases} R(\max(m, j_0) + c_0 + \log_\ell Z), & e \notin \mathcal{E}, \\ Rm + \exp\big((2en)^{C_H} \log(2|\Delta_{L_{j_0}}|)\big)/\log \ell, & e \in \mathcal{E}. \end{cases}$$

The set $\mathcal{E}$ depends on Z but not on m. The first bound is logarithmic in Z; the second is affordable only when e is a small power of the scale, by Problems 54.4.1 and 54.4.2. The exceptional twists cannot be moved, so the scale must be moved: this is the origin of the windows.

In the Lean formalization. In [Lean] a layer is `IsLayer`; Problems 54.1.1–54.1.5 correspond to `exists_cyclotomic_layer_of_primitiveRoot`, `layeriso`, `rootdeg`, `disc` and `layerdisc`. Theorem 54.3.1 is `Published.FerreroWashington`, proved by `FW.ferreroWashington`. The hypothesis of Lemma 54.3.2 is `Tower.IsTower`; parts (a) and (b) are the two clauses of `Win.ABound`, the second being `SecondBound`, and the lemma is `PropA.aBound_of_isTower`; j_0 is `jZero`. The identity (1) is the statement `VFormula`. Theorem 54.4.1 is `LemmaK`, supplied by `lemmaK_of_litN_alt` through `BOdd`. Problem 54.2.4 is `Win.exc` with `FirstBound`, and Theorem 54.4.2 combines it with `Win.point`.

Hints

§54.1.

54.1.1: The cyclotomic character embeds $\mathrm{Gal}(L_\infty/L_0)$ as an infinite closed subgroup of $1 + \ell\mathbb{Z}_\ell$ (of $1 + 4\mathbb{Z}_2$ if $\ell = 2$).
54.1.2: Complex conjugation.
54.1.3: $\varphi(\ell^k) \le [L:\mathbb{Q}]$.
54.1.4: The conductor–discriminant formula [Wa, Ch. 3].
54.1.5: $L \subseteq \mathbb{Q}(\zeta_{\ell^k N_0 P})$; apply Problems 54.1.3 and 54.1.4.

§54.2.

54.2.1: $v_\ell(\log \kappa) = 1$, and exp preserves valuations on $\ell\mathbb{Z}_\ell$.
54.2.2: Problem 54.2.1.
54.2.3: The length of the cokernel of an injective endomorphism of $\mathbb{Z}_\ell^r$ is the valuation of its determinant.

54.2.4: The ultrametric inequality, applied to the difference of two such integers.

54.2.6: Kummer's congruences: for $k \not\equiv 0 \pmod{36}$, $(1 - 37^{k-1})B_k/k \bmod 37^n$ depends only on $k \bmod 36 \cdot 37^{n-1}$ [Wa, Ch. 5]. Compute $v_{37}(B_k/k)$ for one k in each class.

54.2.7: Problem 30.2.1.

§54.3.

54.3.1: Modulo ℓ, $\omega_m \equiv T^{\ell^m}$; bound $\dim X/\ell X$, then use Nakayama's lemma for compact $\mathbb{Z}_\ell$-modules.

54.3.2: The image of the cyclotomic character.

54.3.3: The identity (1).

§54.4.

54.4.2: Compare logarithms; $\log(2|\Delta_L|) \geq \log 2$.

References

[FW] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), 377–395.

[Lean] The Lean community, *riemann-hypothesis*, a Lean formalization of Alpöge's argument, `https://github.com/leanprover-community/riemann-hypothesis`.

[NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, 2008.

[Rub] *The Alpöge–Claude proof of the Riemann hypothesis explained for the Riemann zeta function*, written by AI models at the behest of M. O. Rubinstein, working draft, 21 November 2026, `https://www.math.uwaterloo.ca/~mrubinst/alpoge_claude_grh/zeta-paper.pdf`.

[Si] W. Sinnott, *On the μ-invariant of the Γ-transform of a rational function*, Invent. Math. **75** (1984), 273–282.

[So79] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979), 251–295.

[So03] C. Soulé, *A bound for the torsion in the K-theory of algebraic integers*, Doc. Math. Extra Vol. Kazuya Kato's Fiftieth Birthday (2003), 761–788.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

[Zh] R. Zhang, *A preliminary note on Alpöge's proposed proof of the generalized Riemann hypothesis*, 22 November 2026, `https://hexagonmath.org/pdf/2611.00809v1`.