DEFORMALIZATION 1

Twisted cokernels in a cyclotomic tower

One cluster of the Lean archive behind the proof of the Riemann hypothesis announced by L. Alpöge, read back into mathematics

Summary. Let X be a module over the ℓ-adic integers generated by R elements, γ an endomorphism of X that is unipotent modulo ℓ, and $u \neq 1$ an element of $1 + \ell\mathbb{Z}_\ell$ (of $1 + 4\mathbb{Z}_2$ if $\ell = 2$). We study the lengths $\tau(\gamma, u; h, m)$ of the cokernels of $(u^h\gamma)^{\ell^m} - 1$ as the *twist* h and the *layer* m vary. There are R points $c_1, \dots, c_R$ of $\mathbb{Z}_\ell$, the *centres*, such that $\tau(\gamma, u; h, m)$ exceeds a quantity depending only on the layer by at most $\sum_i v_\ell(c_i - h)$, where $v_\ell(x)$ is the ℓ-adic valuation of x. Hence among the twists $1 \le h \le Z$ at most R are exceptional, however large Z is. Applied to the Iwasawa module of the cyclotomic $\mathbb{Z}_\ell$-extension of a number field, this bounds the locally trivial cohomology of the Tate twists of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ along the tower. The proof is linear algebra over $\mathbb{Z}_\ell$ and one compactness argument; it uses neither the structure theorem for Iwasawa modules nor the ℓ-adic logarithm.

What this note is. On 20 November 2026 L. Alpöge announced a proof of the Riemann hypothesis, with a Lean archive [Al]. That is a claim, and nothing here asserts that the hypothesis is proved. This note takes one cluster of the archive, the 4 declarations that the embedding atlas [At] groups as *Assemble the arithmetic tower window*, together with the directory on which they rest (29 files, 1,193 lines, 42 theorems and lemmas), and rewrites it as mathematics. The algebra is proved in full (§3–§6 and Proposition 7.9). Of the three arithmetic inputs (§7), two are stated with a sketch, and the third, the descent to a layer of the tower, is proved in §8 from two statements of a neighbouring directory. Every statement was compared with its formal counterpart at commit `40e56bab` of the public mirror; Appendix A is the concordance of 108 declarations. Formal status: 3 of the 4 declarations were replayed by name by the reading project (type, axioms, kernel), the fourth lies in the closure of one of them. The complete proof, of which the cluster is a part, is the subject of the replays recorded in the ledger of this project.

1 The question

In the announced argument a chain of theta lifts is compared with a sum over primes, and each lift loses a factor. For a prime ℓ the loss is governed by groups of Galois cohomology: for a number field E and an integer $h \ge 1$, by the length of the group $Ш^1_\ell(E, h)$ of classes with coefficients in the $(-h)$-th Tate twist of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ that are unramified outside ℓ and trivial at the places above ℓ (the definition is recalled in §7). The proof needs the total length over all twists $1 \le h \le Z$, for a very large Z, to be small on a whole range of scales; see §6 of the guide [Gu]. A bound for each h that grows with Z is useless. What one can hope for is a bound that holds for all twists except a set of *exceptional* ones, *whose number does not depend on Z*.

Along the cyclotomic tower over E these lengths are lengths of cokernels of one operator on one module. This note proves the statement about exceptional twists for such operators, in the generality in which the archive proves it.

The simplest case. Let $X = \mathbb{Z}_\ell$, with ℓ odd, let $u = 1 + \ell$, and let γ be multiplication by a principal unit, which we write as u^{-c} with $c \in \mathbb{Z}_\ell$. For integers $h, m \geq 0$ the operator $(u^h\gamma)^{\ell^m} - 1$ is multiplication by $u^{\ell^m(h-c)} - 1$, an element of valuation $1 + m + v_\ell(h - c)$. So the cokernel has length

$$\tau(\gamma, u; h, m) = 1 + m + v_\ell(h - c).$$

It is large only when the integer h is ℓ-adically close to c. Now two integers $1 \leq h < h' \leq Z$ cannot both satisfy $v_\ell(h - c) > \log_\ell Z$: their difference would be divisible by a power of ℓ larger than Z. So at most one twist $h \leq Z$ is exceptional, whatever Z. The general case has R eigenvalues in place of one, hence R centres; the work lies in doing without a diagonal form, and in allowing torsion in X.

2 Setting and results

Conventions. Throughout, ℓ is a prime number, $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers, $\mathbb{Q}_\ell$ its field of fractions and $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$. A *module* is a module over $\mathbb{Z}_\ell$, unless another ring is named, and the letters X, M and D stand for modules. The *length* $\operatorname{len} M$ of a module M is the supremum of the lengths of its chains of submodules, a non-negative integer or ∞; it is additive in short exact sequences, so the length of a submodule or of a quotient of M is at most $\operatorname{len} M$. A finite module of order ℓ^n has length n. We write $\operatorname{End}(X)$ for the ring of endomorphisms of X, 1 for the identity, and identify a scalar with the multiplication by it. In §7 and §8 the letters F and L stand for number fields, and a field with a bar for an algebraic closure of the field.

Definition 2.1 (valuation). For $x \in \mathbb{Z}_\ell$ the *ℓ-adic valuation* $v_\ell(x)$ is the largest integer $n \geq 0$ with $x \in \ell^n\mathbb{Z}_\ell$, and $v_\ell(0) = \infty$; thus $v_\ell(\ell) = 1$. It is a function of the prime and of x, and both are written every time. The same notation is used for the extension of the valuation to $z \in \overline{\mathbb{Q}}_\ell$, and $|z| = \ell^{-v_\ell(z)}$ is the absolute value. It is ultrametric: $|z + z'| \leq \max(|z|, |z'|)$.

LEAN `vl`

Definition 2.2 (generators). Let X be a module and $R \geq 0$ an integer. The module X is *generated by R elements* if there is a surjective homomorphism of modules $\pi : \mathbb{Z}_\ell^R \to X$. No such R is fixed in this note, and every statement names its own.

LEAN `GenBy`

Definition 2.3 (cokernels and congruences). Let X be a module and $f \in \operatorname{End}(X)$. The cokernel of f is

$$\operatorname{cok} f = X/f(X),$$

and $\operatorname{len}\operatorname{cok} f$, an element of $\{0, 1, 2, \dots, \infty\}$, is the length of the cokernel of f. For an integer $n \geq 0$ we write $f \equiv 0 \pmod{\ell^n}$ if $f(X) \subseteq \ell^n X$, and $f \equiv g \pmod{\ell^n}$, for $g \in \operatorname{End}(X)$, if $f - g \equiv 0 \pmod{\ell^n}$. The set I_n of the $f \in \operatorname{End}(X)$ with $f \equiv 0 \pmod{\ell^n}$ is a two-sided ideal, $I_i I_j \subseteq I_{i+j}$, and it contains $\ell^n \operatorname{End}(X)$. (If X has torsion, I_n can be larger than $\ell^n \operatorname{End}(X)$.)

LEAN `cokLen` · `InPow`

Definition 2.4. Let X be a module. An endomorphism γ of X is *unipotent modulo ℓ* if $(\gamma - 1)^k \equiv 0 \pmod{\ell}$ for some integer $k \geq 1$.

LEAN `Unip`

Definition 2.5. An element u of $\mathbb{Z}_\ell$ has *level* a, for an integer $a \geq 1$, if $v_\ell(u-1) = a$, and $a \geq 2$ in case $\ell = 2$. Such a u is a unit, and it generates the group $1 + \ell^a\mathbb{Z}_\ell$ topologically: this group is the closure of the set of powers of u (Lemma 8.3).

LEAN `IsLevel`

Definition 2.6. Let X be a module, $\gamma \in \mathrm{End}(X)$ and $u \in \mathbb{Z}_\ell$. For integers $h, m \geq 0$, the *twisted length* of the pair (γ, u) at twist h and layer m is

$$\tau(\gamma, u; h, m) = \operatorname{len}\operatorname{cok}\big((u^h\gamma)^{\ell^m} - 1\big) \ \in \ \{0, 1, 2, \dots, \infty\}.$$

It is a function of four arguments, and all four are written every time: the endomorphism and the scalar are never dropped from the notation. The definition asks nothing of γ and u; unipotence and the level are hypotheses of the theorems below, not of the definition.

For integers $R \geq 0$ the *reference layer* is $m_0(\ell, R) = \lfloor \log_\ell R \rfloor + 3$, with $m_0(\ell, 0) = 3$. It depends on the prime and on R only.

LEAN `twLen` · `jZero`

Results. The three statements that follow have the same hypotheses. They are written out once, and each statement cites them.

Setting 2.7. X is a module generated by R elements, for an integer $R \geq 0$; γ is an endomorphism of X that is unipotent modulo ℓ; and u is an element of $\mathbb{Z}_\ell$ of level a, for an integer $a \geq 1$.

Theorem A (centres). *In Setting 2.7 there are $c_1, \dots, c_R \in \mathbb{Z}_\ell$, chosen for the pair (γ, u) and the same for all twists and layers, such that for all integers $h, m \geq 0$*

$$\tau(\gamma, u; h, m) \ \leq \ \sum_{i=1}^{R} \Big(\max\big(m, m_0(\ell, R)\big) + a + v_\ell(c_i - h) \Big).$$

Theorem B (growth). *In Setting 2.7, for all integers $h, m \geq 0$*

$$\tau(\gamma, u; h, m) \ \leq \ \tau(\gamma, u; h, m_0(\ell, R)) + R \cdot \max\big(m - m_0(\ell, R), 0\big).$$

Corollary C (exceptional twists). *In Setting 2.7, let $c_1, \dots, c_R$ be centres of the pair (γ, u) as in Theorem A, and let $Z \geq 1$ be an integer. The set $\mathscr{E}_Z$ of integers $1 \leq h \leq Z$ such that $v_\ell(c_i - h) > \lfloor \log_\ell Z \rfloor$ for some i has at most R elements. For every integer $1 \leq h \leq Z$ outside $\mathscr{E}_Z$ and every $m \geq 0$*

$$\tau(\gamma, u; h, m) \ \leq \ R\,\big(\max\big(m, m_0(\ell, R)\big) + a + \lfloor \log_\ell Z \rfloor\big).$$

LEAN A `exists_centres` · B `twLen_le_growth` · C: the bound `exists_centres_norm`, with `vl_le_of_norm`; the count is proved in the archive for the lengths of Theorem D (Corollary 7.14)

The order of the choices matters. The module, the endomorphism γ and the scalar u are given first; the centres are then chosen for them, and a different γ or a different u has different centres. Only after that do the twist h and the layer m vary. In §7 the pair (γ, u) is

a particular one: the action of an element σ of a Galois group on the Iwasawa module, and the value of the cyclotomic character at σ.

The two theorems complement each other. Theorem A is strong when h is far from every centre, and says nothing when h is a centre: then its right-hand side is infinite, and $\tau(\gamma, u; h, m)$ may be infinite too (Example 9.1). Theorem B gives no information on any single layer, but it shows that all the layers are controlled by one of them, also at a centre. In the arithmetic application that one layer is bounded by a duality theorem, which is why both are needed.

The arithmetic statement concerns a number field L that contains the ℓ-th roots of unity (the fourth roots if $\ell = 2$), the layers L_m of its cyclotomic $\mathbb{Z}_\ell$-extension, and an Iwasawa module: the Galois group of the maximal abelian pro-ℓ extension of $L_\infty = \bigcup_m L_m$ that is unramified everywhere and in which every prime above ℓ splits completely. In the archive this module is a function of three arguments, written $X_\infty(\ell, N, U)$ here (Definition 7.3): the prime, an integer N whose prime divisors are the places where complete splitting is asked, and a subgroup U of the Galois group. The module of the theorem is the one with $N = \ell$ and with U the whole group. The fields are set up in Setting 7.4 of §7, the three statements of Galois cohomology that the archive assumes are listed in Setting 7.8, and the theorem cites both.

Theorem D (class groups in the tower). *In Setting 7.4, with the number field L, its algebraic closure $\overline{L}$ and the layers L_m of that setting, assume the three hypotheses on Galois cohomology of Setting 7.8. Write $G = \mathrm{Gal}(\overline{L}/L)$ and $a = a_\ell(L)$ (Definition 7.2), and suppose that the module $X_\infty(\ell, \ell, G)$ is generated by $R \geq 1$ elements. Then*

(i) *there are $c_1, \dots, c_R \in \mathbb{Z}_\ell$, depending on L, such that for all integers $h \geq 1$ and $m, B \geq 0$ with $v_\ell(c_i - h) \leq B$ for all i*

$$\operatorname{len} Ш^1_\ell(L_m, h) \;\leq\; R\big(\max\big(m, m_0(\ell, R)\big) + a + B\big);$$

(ii) *for all integers $h \geq 1$ and $m \geq 0$, writing $n = m_0(\ell, R)$ for the reference layer, and for every local datum $\mathscr{D}$ of the field L_n at ℓ (Definition 7.7),*

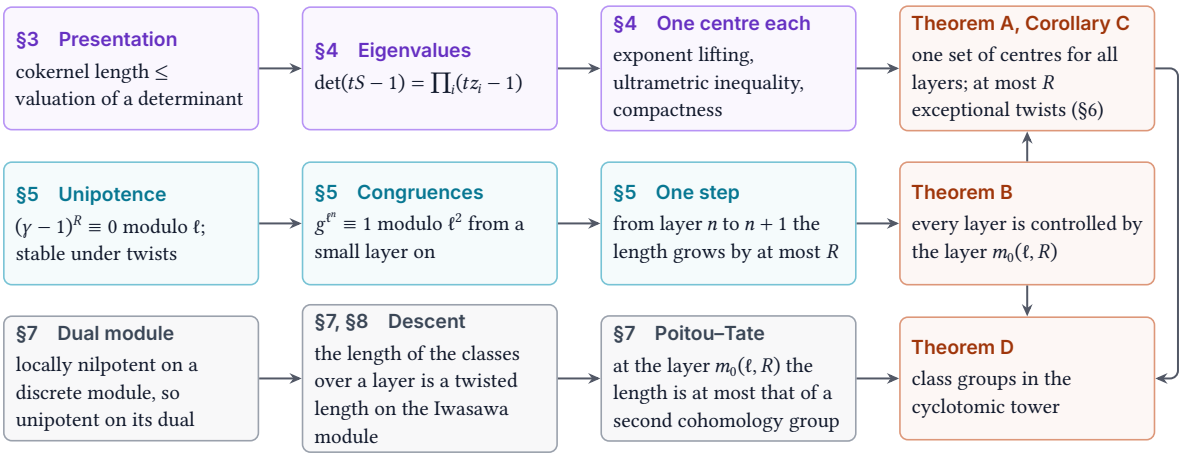
$$\operatorname{len} Ш^1_\ell(L_m, h) \;\leq\; \operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big) + R \cdot \max(m - n, 0).$$

In particular the tower bound of Definition 7.12 holds for (ℓ, R, L).

LEAN `aBound_of_isTower` · hypothesis `Tower.IsTower` · the conclusion in the form of the archive: `Win.ABound`, `Win.SecondBound` (Definition 7.12) · the same conclusion from one descending element: `aBound_of_descends` (Proposition 7.11)

Here $\operatorname{len} Ш^1_\ell(F, h)$ is the length of the group of classes of §1 for a number field F (Definition 7.6), and $\operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big)$ is the length of a second cohomology group (Definition 7.7). The three hypotheses of Setting 7.8 (global duality of Poitou and Tate, finiteness of local cohomology, local Tate duality) enter only through Input 3 of §7.

Plan of the proof. The diagram shows the steps in the order in which they are used. The upper row produces the centres at one layer; the middle row compares the layers; the lower row is the dictionary with arithmetic.



The cluster on the map. The embedding atlas [At] places the 818,755 written theorems and lemmas of the archive on a map of mathematical subjects and groups them into 4,983 clusters. The cluster treated here has 4 members: Theorem D in two forms, and two statements that assemble it into the window of the guide (§7). The 42 theorems and lemmas of the directory that proves Theorem D are filed by the atlas under 9 subjects:

Divisibility, congruences and arithmetic functions	13
Matrices, determinants and linear algebra	13
Automorphic representations, trace formulae and theta lifting	4
Galois and profinite cohomology	4
Global fields, idèles and class groups	2
Iwasawa theory and cyclotomic class-group towers	2
p-adic arithmetic and power series	2
Commutative algebra, ideals and modules	1
Local fields, valuation and ramification	1

The first two rows, more than half of the directory, are the algebra of §3–§6 and of Proposition 7.9. The statement is one of Galois cohomology and Iwasawa theory, and almost all of its proof is linear algebra and congruences. A map of subjects shows where the pieces lie; the order in which they are used is the diagram above. (Four of the algebraic lemmas of §5 and §7 are filed under automorphic representations, by the context of their module.)

3 Lengths and determinants

Lemma 3.1. *Let X be a module over $\mathbb{Z}_\ell$ and let $f, g \in \mathrm{End}(X)$.*

(a) *If $g(X) \subseteq f(X)$, then* $\operatorname{len}\operatorname{cok} f \le \operatorname{len}\operatorname{cok} g$.

(b) $\operatorname{len}\operatorname{cok}(fg) \le \operatorname{len}\operatorname{cok} f + \operatorname{len}\operatorname{cok} g$.

(c) *If $i, j \ge 0$ are integers and i divides j, then* $\operatorname{len}\operatorname{cok}(g^i - 1) \le \operatorname{len}\operatorname{cok}(g^j - 1)$.

Proof. (a) $\operatorname{cok} f$ is a quotient of $\operatorname{cok} g$. (b) The module $X/fg(X)$ has the submodule $f(X)/fg(X)$ with quotient $X/f(X)$, and f induces a surjection of $X/g(X)$ onto $f(X)/fg(X)$. (c) If $j = ik$, the factorization $g^j - 1 = (g^i - 1)(1 + g^i + \cdots + g^{i(k-1)})$ shows that the image of $g^j - 1$ lies in that of $g^i - 1$; apply (a). For $j = 0$ the right-hand side is the length of X. □

LEAN (a) `cokLen_le_of_range_le` · (b) `Base.lenComp`, which also has the same inequality for kernels and holds over any commutative ring · (c) `mono`

Lemma 3.2. *For a square matrix A with entries in $\mathbb{Z}_\ell$, of size R,* $\operatorname{len} \mathbb{Z}_\ell^R / A\mathbb{Z}_\ell^R = v_\ell(\det A)$.

Proof. By the theory of elementary divisors there are invertible matrices P, Q over $\mathbb{Z}_\ell$ with $PAQ = \operatorname{diag}(d_1, \dots, d_R)$. The cokernel of A is isomorphic to $\bigoplus_i \mathbb{Z}_\ell/d_i\mathbb{Z}_\ell$, the module $\mathbb{Z}_\ell/d_i\mathbb{Z}_\ell$ has length $v_\ell(d_i)$, and $v_\ell(\det A) = \sum_i v_\ell(d_i)$. Both sides are infinite when $\det A = 0$. □

LEAN `length_cokernel_eq_addVal_det`, there for a square matrix over any discrete valuation ring

Proposition 3.3 (presentation). *Let X be a module generated by R elements and let $g \in \operatorname{End}(X)$. There is a square matrix S over $\mathbb{Z}_\ell$, of size R, such that for every $t \in \mathbb{Z}_\ell$*

$$\operatorname{len} \operatorname{cok}(tg - 1) \;\le\; v_\ell\big(\det(tS - 1)\big).$$

Proof. Let $\pi : \mathbb{Z}_\ell^R \to X$ be a surjection. Lifting the images under $g \circ \pi$ of the basis vectors gives a matrix S with $\pi \circ S = g \circ \pi$. Then $\pi \circ (tS - 1) = (tg - 1) \circ \pi$, so π maps the image of $tS - 1$ into the image of $tg - 1$ and induces a surjection of $\mathbb{Z}_\ell^R/(tS - 1)\mathbb{Z}_\ell^R$ onto $\operatorname{cok}(tg - 1)$. Apply Lemma 3.2. □

LEAN `lift`

Remark 3.4. The inequality is an equality when X is free of rank R, and can be far from one otherwise. For $X = \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$, $g = 1$ and $t \equiv 1 \pmod{\ell}$ the left-hand side is 1 and the right-hand side, for the lift $S = 1$, is $v_\ell(t - 1)$. Determinants see a presentation of the module, not the module.

4 A centre for every eigenvalue

Lemma 4.1 (lifting the exponent). *Let $u \in \mathbb{Z}_\ell$ have level a. Then $v_\ell(u^n - 1) = a + v_\ell(n)$ for every integer n. Consequently, for all integers $j, n, n' \ge 0$,*

$$\left|u^{\ell^j n} - u^{\ell^j n'}\right| = \ell^{-(j+a)}\,|n - n'|.$$

The first formula is the case of the discrete valuation ring $\mathbb{Z}_\ell$, which has characteristic zero and whose maximal ideal contains the prime ℓ, of a statement of the archive on such rings: there the hypothesis on a unit u congruent to 1 is $v_\ell(\ell) < (\ell - 1)\,v_\ell(u - 1)$, with the valuation of the ring, and for $\mathbb{Z}_\ell$ it says that u has a level.

Proof. Write $u = 1 + x$, so $v_\ell(x) = a$. If ℓ does not divide n, then $u^n - 1 = nx + x^2(\cdots)$ has valuation a. For $n = \ell$,

$$u^\ell - 1 = \ell x + \sum_{1<i<\ell} \binom{\ell}{i} x^i + x^\ell,$$

where the first term has valuation $a + 1$, the middle terms have valuation at least $2a + 1$, and the last has valuation ℓa, which exceeds $a + 1$ because $(\ell - 1)a > 1$. This is where $a \ge 2$ is needed for $\ell = 2$. So u^ℓ has level $a + 1$, and induction on $v_\ell(n)$ gives the formula for $n > 0$. For $n < 0$ use $u^n - 1 = -u^n(u^{-n} - 1)$; for $n = 0$ both sides are infinite. The second formula follows from $u^{\ell^j n} - u^{\ell^j n'} = u^{\ell^j n'}(u^{\ell^j (n - n')} - 1)$. □

LEAN `abelian₂.lte` · `lteNorm`, with `norm_le_of_dvd'` and `norm_eq_of_addVal`

Lemma 4.2. *Let t and t' be units of $\mathbb{Z}_\ell$ and $z \in \overline{\mathbb{Q}}_\ell$. Then* $|t - t'| \le \max\big(|tz - 1|,\, |t'z - 1|\big)$.

Proof. We have $(tz - 1) - (t'z - 1) = (t - t')z$. If $|z| \ge 1$, then $|t - t'| \le |(t - t')z|$, and the ultrametric inequality gives the claim. If $|z| < 1$, then $|tz| < 1$, so $|tz - 1| = 1 \ge |t - t'|$. □

LEAN `padic_units_distance_le_max`

Lemma 4.3. *For $n = 0, 1, 2, \ldots$ let $b_n \in \mathbb{Z}_\ell$ and a real number $r_n \geq 0$ be given, such that*

$$|b_n - b_{n'}| \leq \max(r_n, r_{n'}) \qquad \text{for all } n, n'.$$

Then there is $c \in \mathbb{Z}_\ell$ with $|c - b_n| \leq r_n$ for all n.

Proof. The closed balls $\{y : |y - b_n| \leq r_n\}$ are closed subsets of the compact space $\mathbb{Z}_\ell$. Any finitely many of them have a common point, namely the centre b_n of one of smallest radius among them. Hence all of them have a common point. □

LEAN `helly`

Proposition 4.4 (one centre). *Let $u \in \mathbb{Z}_\ell$ have level a, let $j \geq 0$ be an integer and $z \in \overline{\mathbb{Q}}_\ell$. There is $c \in \mathbb{Z}_\ell$ such that for every integer $h \geq 0$*

$$\ell^{-(j+a)}\,|c - h| \;\leq\; \left|u^{\ell^j h} z - 1\right|.$$

Proof. Put $b_h = h$ and $r_h = \ell^{j+a}\,|u^{\ell^j h} z - 1|$. By Lemma 4.1 and Lemma 4.2, applied to the units $u^{\ell^j h}$ and $u^{\ell^j h'}$,

$$|h - h'| = \ell^{j+a}\left|u^{\ell^j h} - u^{\ell^j h'}\right| \leq \max(r_h, r_{h'}).$$

Lemma 4.3 gives c. □

LEAN `ball`

The proposition says that the function $h \mapsto u^{\ell^j h} z - 1$, on the integers, is bounded below by a multiple of the distance to one point. The function extends continuously to $\mathbb{Z}_\ell$. If the extension has a zero c, this zero is the only possible centre, and the inequality is an equality. In general there is no zero in $\mathbb{Z}_\ell$; then the function is bounded away from zero, and the centre is not unique.

Lemma 4.5. *Let S be a square matrix of size R over an algebraically closed field, with eigenvalues $z_1, \ldots, z_R$ counted with multiplicity. Then $\det(tS - 1) = \prod_{i=1}^{R}(tz_i - 1)$ for every element t of the field.*

Proof. S is conjugate to an upper triangular matrix with diagonal $z_1, \ldots, z_R$, and then $tS - 1$ is conjugate to an upper triangular matrix with diagonal $tz_1 - 1, \ldots, tz_R - 1$. □

LEAN `detFactor`

Proposition 4.6. *Let $u \in \mathbb{Z}_\ell$ have level a, let $j \geq 0$, and let S be a square matrix of size R over $\mathbb{Z}_\ell$. There are $c_1, \ldots, c_R \in \mathbb{Z}_\ell$ such that for every integer $h \geq 0$*

$$v_\ell\Big(\det\big(u^{\ell^j h} S - 1\big)\Big) \;\leq\; \sum_{i=1}^{R}\big(j + a + v_\ell(c_i - h)\big).$$

Proof. Let $z_1, \ldots, z_R \in \overline{\mathbb{Q}}_\ell$ be the eigenvalues of S and let c_i be a centre for z_i as in Proposition 4.4. By Lemma 4.5,

$$\Big|\det\big(u^{\ell^j h} S - 1\big)\Big| = \prod_{i=1}^{R}\left|u^{\ell^j h} z_i - 1\right| \;\geq\; \prod_{i=1}^{R} \ell^{-(j+a)}\,|c_i - h|,$$

and taking valuations gives the claim. □

LEAN `detBound` · `normVal`, with `dvd_of_norm_le'` and `vl_prod`

Corollary 4.7 (centres at one layer). *Let X be a module generated by R elements, let γ be any endomorphism of X, let $u \in \mathbb{Z}_\ell$ have level a and let $j \geq 0$. There are $c_1, \dots, c_R \in \mathbb{Z}_\ell$ such that for every integer $h \geq 0$*

$$\tau(\gamma, u; h, j) \;\leq\; \sum_{i=1}^{R} \bigl(j + a + v_\ell(c_i - h)\bigr).$$

Proof. Since $(u^h\gamma)^{\ell^j} = u^{\ell^j h}\gamma^{\ell^j}$, Proposition 3.3 for $g = \gamma^{\ell^j}$ and $t = u^{\ell^j h}$ bounds $\tau(\gamma, u; h, j)$ by $v_\ell(\det(u^{\ell^j h}S - 1))$, with a matrix S that does not depend on h. Apply Proposition 4.6. □

LEAN `exists_centres_level`

Unipotence is not used here. But the matrix S, and with it the centres, depend on the layer j. To have one set of centres for all layers, the layers must be compared. This is the purpose of the next section.

5 Growth along the tower

Lemma 5.1. (a) *If the module X is generated by R elements, then* $\operatorname{len} X/\ell X \leq R$*; in the notation of Definition 2.3 this is* $\operatorname{len}\operatorname{cok}(\ell \cdot 1) \leq R$.

(b) *Let M be a module over a commutative ring, of length at most n for an integer $n \geq 0$. A nilpotent endomorphism f of M satisfies $f^n = 0$.*

Proof. (a) $X/\ell X$ is a quotient of $(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^R$. (b) As long as $f^i \neq 0$, the image of f^{i+1} is strictly smaller than the image of f^i: equality would give $f^i(M) = f^{i+j}(M)$ for all j, hence $f^i = 0$. If $f^n \neq 0$, the images of $f^0, f^1, \dots, f^n$ and the zero module would form a chain of length $n + 1$. □

LEAN `cokL` · `nilLen`, with `nilLen_range_succ` and `nilLen_lt`

Lemma 5.2. *Let X be a module generated by R elements and let $\gamma \in \operatorname{End}(X)$ be unipotent modulo ℓ.*

(a) $(\gamma - 1)^R \equiv 0 \pmod{\ell}$.

(b) *For every $t \in \mathbb{Z}_\ell$ with $t \equiv 1 \pmod{\ell}$, the endomorphism $t\gamma$ is unipotent modulo ℓ.*

Proof. (a) The endomorphism of $X/\ell X$ induced by $\gamma - 1$ is nilpotent, and $X/\ell X$ has length at most R; apply Lemma 5.1. (b) Write $t\gamma - 1 = (\gamma - 1) + (t - 1)\gamma$. The two summands commute and the second lies in I_1. In the binomial expansion of $(t\gamma - 1)^k$ every term except $(\gamma - 1)^k$ contains the second summand, so it lies in the ideal I_1; and $(\gamma - 1)^k \in I_1$ for a suitable k. □

LEAN `unipPow` · `twist`

Lemma 5.3 (congruences). *Let X be a module, let $g, w \in \operatorname{End}(X)$ and let $k, n \geq 0$ be integers.*

(a) $(g - 1)^{\ell^k} \equiv g^{\ell^k} - 1 \pmod{\ell}$.

(b) *If $w \equiv 1 \pmod{\ell^n}$, then $w^i \equiv 1 \pmod{\ell^n}$ for every $i \geq 0$.*

(c) *If $w \equiv 1 \pmod{\ell}$, then $w^\ell \equiv 1 \pmod{\ell^2}$.*

Proof. (a) The polynomial $(T - 1)^{\ell^k} - (T^{\ell^k} - 1)$ has coefficients divisible by ℓ. (b) We have $w^i - 1 = (1 + w + \cdots + w^{i-1})(w - 1)$, and I_n is an ideal. (c) Put $f = w - 1 \in I_1$. In $w^\ell - 1 = \sum_{i=1}^{\ell} \binom{\ell}{i} f^i$ the terms with $i < \ell$ lie in $\ell I_1 \subseteq I_2$, and $f^\ell \in I_\ell \subseteq I_2$. □

LEAN `frob` · `powIn`

Lemma 5.4 (one step). *Let X be a module generated by R elements and let $w \in \mathrm{End}(X)$ with $w \equiv 1 \pmod{\ell^2}$. Put $v = 1 + w + \cdots + w^{\ell-1}$. Then $\ell X \subseteq v(X)$, and*

$$\operatorname{len}\operatorname{cok}(w^\ell - 1) \;\le\; \operatorname{len}\operatorname{cok}(w - 1) + R.$$

Proof. We have $w^\ell - 1 = v(w-1)$. By Lemma 5.3(b) each w^i is congruent to 1 modulo ℓ^2, so $v \equiv \ell \pmod{\ell^2}$: for every $x \in X$ there is y with $\ell x = vx - \ell^2 y$. Thus $\ell X \subseteq v(X) + \ell \cdot \ell X$. The module ℓX is finitely generated, so Nakayama's lemma gives $\ell X \subseteq v(X)$. By Lemma 3.1(a) and Lemma 5.1(a), $\operatorname{len}\operatorname{cok} v \le \operatorname{len} X/\ell X \le R$, and Lemma 3.1(b) finishes the proof. □

LEAN the inclusion `phi`, there for every finitely generated module · the inequality `step`

Proposition 5.5 (growth). *Let X be a module generated by R elements and let $g \in \mathrm{End}(X)$ be unipotent modulo ℓ. Then for every integer $m \ge 0$*

$$\operatorname{len}\operatorname{cok}\bigl(g^{\ell^m} - 1\bigr) \;\le\; \operatorname{len}\operatorname{cok}\bigl(g^{\ell^{m_0(\ell,R)}} - 1\bigr) + R \cdot \max(m - m_0(\ell,R), 0).$$

Proof. For $m \le m_0(\ell,R)$ the exponent ℓ^m divides $\ell^{m_0(\ell,R)}$, and the claim is Lemma 3.1(c).

Let $k = m_0(\ell,R) - 2$, so that $R \le \ell^k$. Then, modulo the indicated powers of ℓ,

$$(g-1)^{\ell^k} \equiv 0\ (\ell), \qquad g^{\ell^k} \equiv 1\ (\ell), \qquad g^{\ell^{k+1}} \equiv 1\ (\ell^2), \qquad g^{\ell^n} \equiv 1\ (\ell^2) \quad \text{for all } n \ge k+1,$$

by Lemma 5.2(a) and parts (a), (c), (b) of Lemma 5.3, in this order. For such n, Lemma 5.4 with $w = g^{\ell^n}$ gives

$$\operatorname{len}\operatorname{cok}\bigl(g^{\ell^{n+1}} - 1\bigr) \;\le\; \operatorname{len}\operatorname{cok}\bigl(g^{\ell^n} - 1\bigr) + R,$$

and the claim for $m > m_0(\ell,R)$ follows by induction, starting from $n = m_0(\ell,R)$. □

LEAN `growth`, with `mono` for the layers below the reference layer

Proof of Theorems A and B. Since $u \equiv 1 \pmod{\ell}$, also $u^h \equiv 1 \pmod{\ell}$, so $u^h\gamma$ is unipotent modulo ℓ by Lemma 5.2(b). Proposition 5.5 for $g = u^h\gamma$ is Theorem B. For Theorem A take the centres of Corollary 4.7 at the layer $j = m_0(\ell,R)$; then by Theorem B

$$\begin{aligned}\tau(\gamma,u;h,m) \;&\le\; \sum_{i=1}^{R}\bigl(m_0(\ell,R) + a + v_\ell(c_i - h)\bigr) + R\cdot\max\bigl(m - m_0(\ell,R),0\bigr)\\ &=\; \sum_{i=1}^{R}\bigl(\max\bigl(m, m_0(\ell,R)\bigr) + a + v_\ell(c_i - h)\bigr).\end{aligned}$$

□

6 Exceptional twists

Lemma 6.1 (separation). *Let K be a field with an ultrametric absolute value $|\cdot|$ that extends the ℓ-adic absolute value of $\mathbb{Q}_\ell$, let $c \in K$, and let $Z \ge 1$ be an integer. If integers h and h' with $1 \le h \le Z$ and $1 \le h' \le Z$ satisfy*

$$|c - h| < \ell^{-\lfloor \log_\ell Z \rfloor} \qquad \text{and} \qquad |c - h'| < \ell^{-\lfloor \log_\ell Z \rfloor},$$

then $h = h'$. In particular, for $c \in \mathbb{Z}_\ell$ at most one integer h with $1 \le h \le Z$ satisfies $v_\ell(c-h) > \lfloor \log_\ell Z \rfloor$.

Proof. By the ultrametric inequality $|h' - h| \le \max(|c-h|, |c-h'|) < \ell^{-\lfloor \log_\ell Z \rfloor}$. The absolute value of K restricts to the ℓ-adic one on the integers, so $v_\ell(h'-h) > \lfloor \log_\ell Z \rfloor$: the integer $h' - h$ is divisible by $\ell^{\lfloor \log_\ell Z \rfloor + 1}$, which is larger than Z. But $h' - h$ lies strictly between $-Z$ and Z. So $h' - h = 0$. The last sentence is the case $K = \mathbb{Q}_\ell$, where $|c-h| = \ell^{-v_\ell(c-h)}$. □

LEAN `Win.near1`

Proof of Corollary C. By Lemma 6.1 each centre contributes at most one element to $\mathscr{E}_Z$. If $1 \le h \le Z$ is not in $\mathscr{E}_Z$, then $v_\ell(c_i - h) \le \lfloor \log_\ell Z \rfloor$ for all i, and Theorem A gives the bound. □

In the archive the count of the exceptional twists is stated for the arithmetic lengths of Theorem D, not for abstract modules, and the centres there lie in a field K as in Lemma 6.1; this form is Corollary 7.14 of §7, and the argument is the one above.

7 Class groups in the cyclotomic tower

This section defines the objects of Theorem D, each with all the arguments of its formal definition, states three inputs and proves the theorem. The definitions are made for any number field, as in the archive; the theorem uses them for the field of Setting 7.4.

Galois groups. Let F be a number field and $\overline{F}$ an algebraic closure of F. The group $\mathrm{Gal}(\overline{F}/F)$ of the automorphisms of $\overline{F}$ over F carries the Krull topology; the same notation is used for any Galois extension of F in the place of $\overline{F}$. For a subfield E of $\overline{F}$, which need not contain F, we write $\mathrm{Gal}_F(\overline{F}/E)$ for the subgroup of the elements of $\mathrm{Gal}(\overline{F}/F)$ that fix every element of E. The map

$$\kappa_\ell^{\overline{F}/F}(\cdot) : \quad \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbb{Z}_\ell^\times$$

is the ℓ-adic cyclotomic character: $\sigma(\zeta) = \zeta^u$ with $u = \kappa_\ell^{\overline{F}/F}(\sigma)$, for every root of unity $\zeta \in \overline{F}$ of ℓ-power order. The field, its closure and the prime are part of the notation and are written every time; for a subgroup V we write $\kappa_\ell^{\overline{F}/F}(V)$ for its image. For an integer $n \ge 0$ let

$$U_\ell^{(n)} = \left\{ u \in \mathbb{Z}_\ell^\times \ : \ u \equiv 1 \pmod{\ell^n} \right\},$$

so that $U_\ell^{(0)} = \mathbb{Z}_\ell^\times$ and $U_\ell^{(n)} = 1 + \ell^n \mathbb{Z}_\ell$ for $n \ge 1$. These are closed subgroups of $\mathbb{Z}_\ell^\times$. For a subgroup U of $\mathrm{Gal}(\overline{F}/F)$ put

$$U_{\ell,n} = \left\{ \sigma \in U \ : \ \kappa_\ell^{\overline{F}/F}(\sigma) \in U_\ell^{(n)} \right\}, \qquad U_{\ell,\infty} = \left\{ \sigma \in U \ : \ \kappa_\ell^{\overline{F}/F}(\sigma) = 1 \right\}.$$

For the whole group in the place of U the first of them is also written $\mathrm{Gal}(\overline{F}/F)_{\ell,n}$.

Definition 7.1 (topological generators). Let F be a number field with an algebraic closure $\overline{F}$, let U be a subgroup of $\mathrm{Gal}(\overline{F}/F)$ and $\sigma \in \mathrm{Gal}(\overline{F}/F)$. We say that σ is a *topological generator of U for the cyclotomic character of ℓ* if $\sigma \in U$ and the image $\kappa_\ell^{\overline{F}/F}(U)$ lies in the closure of the set of the powers $\kappa_\ell^{\overline{F}/F}(\sigma)^n$, $n \in \mathbb{Z}$.

LEAN `Tower.IsGen`

Definition 7.2 (the exponent). For a field L, the number $a_\ell(L)$ is the largest integer $n \ge 0$ such that L contains a primitive root of unity of order ℓ^n. A number field contains finitely many roots of unity, so for it such an integer exists. (The archive defines $a_\ell(L)$ as a supremum, for any natural number in place of the prime and any field, and the supremum is read as 0 when the orders are not bounded.)

LEAN `Tower.cZero`

Definition 7.3 (characters with local conditions). Let F be a number field with an algebraic closure $\overline{F}$, let $N \ge 0$ be an integer, U a subgroup of $\mathrm{Gal}(\overline{F}/F)$, Λ a commutative ring and M a

module over Λ. A *valuation ring* of $\overline{F}$ is a subring $\mathcal{O}$ such that $y \in \mathcal{O}$ or $y^{-1} \in \mathcal{O}$ for every non-zero $y \in \overline{F}$. Its *decomposition group* consists of the $\sigma \in \mathrm{Gal}(\overline{F}/F)$ with $\sigma(\mathcal{O}) = \mathcal{O}$, and its *inertia group* of those among them for which $\sigma y - y$ lies in the maximal ideal of $\mathcal{O}$ for every $y \in \mathcal{O}$. We write

$$D_N(U; \Lambda, M)$$

for the Λ-module of the maps $\varphi : U \to M$ with the following four properties.

(1) φ is locally constant.
(2) $\varphi(\rho\rho') = \varphi(\rho) + \varphi(\rho')$ for all $\rho, \rho' \in U$.
(3) φ vanishes on the intersection of U with the inertia group of every valuation ring of $\overline{F}$.
(4) φ vanishes on the intersection of U with the decomposition group of every valuation ring of $\overline{F}$ whose maximal ideal contains N.

For the prime ℓ we put

$$D_\infty(\ell, N, U) = D_N(U_{\ell,\infty}; \mathbb{Z}_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell), \qquad X_\infty(\ell, N, U) = \mathrm{Hom}_{\mathbb{Z}_\ell}\big(D_\infty(\ell, N, U),\ \mathbb{Q}_\ell/\mathbb{Z}_\ell\big).$$

Each of them is a function of three arguments, and all three are written every time. If U is a normal subgroup, $\mathrm{Gal}(\overline{F}/F)$ acts on both modules:

$$(\sigma\varphi)(\rho) = \varphi(\sigma^{-1}\rho\sigma), \qquad (\sigma x)(\varphi) = x(\sigma^{-1}\varphi) \qquad \text{for } \varphi \in D_\infty(\ell, N, U),\ x \in X_\infty(\ell, N, U).$$

LEAN `XDual`

The *Iwasawa module* of Theorem D is $X_\infty(\ell, \ell, \mathrm{Gal}(\overline{L}/L))$, for the field L of Setting 7.4: here $N = \ell$ and U is the whole group. For this U the group $U_{\ell,\infty}$ is $\mathrm{Gal}_L(\overline{L}/L_\infty)$, and $D_\infty(\ell, \ell, \mathrm{Gal}(\overline{L}/L))$ is the group of the continuous homomorphisms $\mathrm{Gal}_L(\overline{L}/L_\infty) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$ that vanish on every inertia group and on the decomposition groups of the places above ℓ. By Pontryagin duality its dual is the Galois group of the maximal abelian pro-ℓ extension of L_∞ that is unramified everywhere and in which the primes above ℓ split completely, as in §2; the archive works with the definition as a dual, which needs no topology on the module. With $N = 1$ no decomposition group enters, and $X_\infty(\ell, 1, \mathrm{Gal}(\overline{L}/L))$ is the Galois group of the maximal unramified abelian pro-ℓ extension of L_∞.

Setting 7.4. L is a number field and $\overline{L}$ is an algebraic closure of L. The field L contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$. Such a field is totally complex (Lemma 8.5(d)); the archive lists this among its hypotheses. The field $L_\infty \subseteq \overline{L}$ is generated over L by all roots of unity of ℓ-power order, and for an integer $m \geq 0$ the field L_m is the subfield of L_∞ of degree ℓ^m over L.

In Setting 7.4 the image of $\mathrm{Gal}(\overline{L}/L)$ under the cyclotomic character is the group $U_\ell^{(a)}$ with $a = a_\ell(L)$, a group isomorphic to $\mathbb{Z}_\ell$, and the field L_m exists and is unique (Lemma 8.6).

Definition 7.5 (layers). Let $j \geq 0$ be an integer and let L' be an extension of a field L. The field L' is a *layer of index j over L for the prime ℓ* if, for some integer $k \geq 0$, it contains a primitive root of unity of order ℓ^k and is generated over L by the roots of unity of order dividing ℓ^k, and if the degree of L' over L is ℓ^j.

LEAN `IsLayer`

In Setting 7.4 the field L_m is a layer of index m over L for ℓ, and a number field that is a layer of index m over L for ℓ is isomorphic to L_m over L (Lemma 8.6). The statements of this note are made for the fields L_m; the archive makes them for every such layer.

Definition 7.6 (the classes and their length). Let F be a number field, $\overline{F}$ an algebraic closure of F and h an integer. The Tate twist $\mathcal{Q}_\ell^{\overline{F}/F}(-h)$ is the group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ on which $\sigma \in \mathrm{Gal}(\overline{F}/F)$ acts as the multiplication by $\kappa_\ell^{\overline{F}/F}(\sigma)^{-h}$; it is a function of the field, its closure, the prime and the twist. A valuation ring of $\overline{F}$ lies *above* a prime $\mathfrak{p}$ of F if its maximal ideal meets the ring of integers of F in $\mathfrak{p}$. The group $Ш^1_\ell(F,h)$ consists of the classes in $H^1\big(\mathrm{Gal}(\overline{F}/F), \mathcal{Q}_\ell^{\overline{F}/F}(-h)\big)$ whose restriction to the decomposition group of every valuation ring above a prime of F that divides ℓ is trivial, and whose restriction to the inertia group of every valuation ring above a prime of F that does not divide ℓ is trivial. Cohomology is that of continuous cochains, for the discrete topology on the coefficients. The length of this group is written

$$\operatorname{len} Ш^1_\ell(F,h) \;\in\; \{0,1,2,\dots,\infty\};$$

it is a function of the field, the prime and the twist.

LEAN `shaInv`

Definition 7.7 (local data). Let F be a number field. A *local datum of F at ℓ* is a pair $\mathscr{D}$ of an algebraic closure $\overline{F}$ of F and of a choice, for every prime $\mathfrak{p}$ of F that divides ℓ, of one valuation ring of $\overline{F}$ above $\mathfrak{p}$. Let $\Gamma_{\mathscr{D}}$ be the quotient of $\mathrm{Gal}(\overline{F}/F)$ by the closed normal subgroup generated by the inertia groups of the valuation rings above the primes of F that do not divide ℓ: the Galois group of the maximal extension of F in $\overline{F}$ that is unramified outside ℓ and the infinite places. The cyclotomic character $\kappa_\ell^{\overline{F}/F}(\cdot)$ factors through $\Gamma_{\mathscr{D}}$. For an integer h let $\mathbb{Z}_\ell(h)$ be the group $\mathbb{Z}_\ell$ on which $\Gamma_{\mathscr{D}}$ acts through the h-th power of this character, and let $\mathcal{Q}(\mathscr{D})(-h)$ be the group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ on which $\Gamma_{\mathscr{D}}$ acts through its $(-h)$-th power, as in Definition 7.6. We write $H^i(\mathscr{D},\cdot)$ for the continuous cohomology of $\Gamma_{\mathscr{D}}$, and

$$Ш^1(\mathscr{D},h) = \ker\Big(H^1\big(\mathscr{D},\mathcal{Q}(\mathscr{D})(-h)\big) \longrightarrow \prod_{\mathfrak{p}\mid\ell} H^1\big(F_\mathfrak{p},\mathcal{Q}(\mathscr{D})(-h)\big)\Big),$$

where the cohomology of the completion $F_\mathfrak{p}$ is that of the decomposition group of the valuation ring chosen above $\mathfrak{p}$. The length of the second cohomology group is written

$$\operatorname{len} H^2\big(\mathscr{D},\mathbb{Z}_\ell(h+1)\big) \;\in\; \{0,1,2,\dots,\infty\};$$

it is a function of the datum and of the twist. The two descriptions of the classes have the same length: for every local datum $\mathscr{D}$ of F at ℓ and every integer h,

$$\operatorname{len} Ш^1(\mathscr{D},h) = \operatorname{len} Ш^1_\ell(F,h).$$

This is a theorem of the archive, proved in a neighbouring directory by inflation; it is not deformalized here.

LEAN `VLen` · the equality of the two lengths `shaLen_eq_shaInv`

Setting 7.8 (three hypotheses on Galois cohomology). The following three statements hold in the form in which the archive states them, for every prime number in the place of ℓ. They are hypotheses of the cluster. They are not deformalized in this note.

(a) *The duality of Poitou and Tate* [NSW, VIII, §6], for a number field that is totally complex if the prime is 2, a finite set of its primes that contains those above the prime, and a finite module of order a power of the prime over the Galois group of the maximal extension unramified outside this set: the exact sequence of nine terms, the duality of the locally trivial classes in degrees 1 and 2, and the vanishing of the cohomology in degrees at least 3.

(b) *Finiteness of local cohomology*: for a finite extension of the field of ℓ-adic numbers and a finite Galois module of order a power of ℓ, the cohomology is finite in degrees 0, 1, 2 and vanishes in degrees at least 3.

(c) *Local Tate duality* for the same modules: the cup products with values in the second cohomology of the roots of unity are perfect pairings.

The algebraic bridge. The module $D_\infty(\ell, N, U)$ is discrete and $X_\infty(\ell, N, U)$ is compact. The next statement passes unipotence from one side to the other. It is pure algebra, and is proved in full in the archive's directory.

Proposition 7.9 (the dual module). *Let D be a module and $g \in \mathrm{End}(D)$. Put*

$$X = \mathrm{Hom}_{\mathbb{Z}_\ell}(D, \mathbb{Q}_\ell/\mathbb{Z}_\ell), \qquad (g^\vee x)(\varphi) = x(g\varphi) \quad \text{for } x \in X,\ \varphi \in D,$$

and let $D[\ell]$ be the submodule of the elements of D killed by ℓ.

(a) *The module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is injective.*

(b) *If X is finitely generated, then $D[\ell]$ is finite.*

(c) *If $x \in X$ vanishes on $D[\ell]$, that is $x(\varphi) = 0$ for all $\varphi \in D$ with $\ell\varphi = 0$, then $x \in \ell X$.*

(d) *Suppose that X is finitely generated and that $g - 1$ is locally nilpotent: for every $\varphi \in D$ there is an integer $k \geq 0$ with $(g-1)^k\varphi = 0$. Then $g^\vee$ is unipotent modulo ℓ.*

Proof. (a) The module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is divisible, hence injective, since $\mathbb{Z}_\ell$ is a principal ideal domain.

(b) Let $x_1, \dots, x_r$ generate X. A non-zero $\varphi \in D[\ell]$ spans a module isomorphic to $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$, which embeds into $\mathbb{Q}_\ell/\mathbb{Z}_\ell$; by injectivity the embedding extends to an element of X that does not vanish at φ. Hence some x_i does not vanish at φ, and $\varphi \mapsto (x_1(\varphi), \dots, x_r(\varphi))$ embeds $D[\ell]$ into the finite group of r-tuples of elements of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ killed by ℓ.

(c) If $x \in X$ vanishes on $D[\ell]$, then $\ell\varphi \mapsto x(\varphi)$ is a well-defined homomorphism $\ell D \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$. By injectivity it extends to some $y \in X$, and $x = \ell y$.

(d) By (b) the module $D[\ell]$ is finite; choose $k \geq 1$ with $(g-1)^k = 0$ on it. For $x \in X$ and $\varphi \in D[\ell]$, $((g^\vee - 1)^k x)(\varphi) = x((g-1)^k\varphi) = 0$. So $(g^\vee - 1)^k x \in \ell X$ by (c). □

LEAN (a) `qzInj` · (b) `torsFin` · (c) `dualDiv` · (d) `dualUnip`

Three inputs. Inputs 1 and 3 are proved in neighbouring directories of the archive, or assumed as hypotheses of the cluster. We state them and indicate the standard arguments; they are not deformalized here. Input 2 is proved in §8. Inputs 1 and 2 are stated for the modules of Theorem D; the archive proves Input 1 for every $D_\infty(\ell, N, U)$ with U closed and normal.

Input 1 (local nilpotence). *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$, and let $\sigma \in G$ satisfy $\kappa_\ell^{\overline{L}/L}(\sigma) \equiv 1 \pmod{\ell}$. Then $\sigma - 1$ is locally nilpotent on $D_\infty(\ell, \ell, G)$: for every $\varphi \in D_\infty(\ell, \ell, G)$ there is an integer $k \geq 0$ with $(\sigma - 1)^k \varphi = 0$.*

Input 2 (descent). *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$, let $\sigma \in G$ be a topological generator of G for the cyclotomic character of ℓ (Definition 7.1), and put $u = \kappa_\ell^{\overline{L}/L}(\sigma)$. For all integers $h \neq 0$ and $m \geq 0$, and for the layer L_m of index m over L,*

$$\operatorname{len} Ш^1_\ell(L_m, h) = \operatorname{len} \operatorname{cok}\big((u^h\sigma)^{\ell^m} - 1\big),$$

where $u^h\sigma$ is the operator on $X_\infty(\ell, \ell, G)$ by which σ acts on the twisted module $X_\infty(\ell, \ell, G)(h)$ of Definition 8.7. For $h \geq 1$ the right-hand side is the twisted length $\tau(\gamma, u; h, m)$ of the pair (γ, u), where γ is the action of σ on $X_\infty(\ell, \ell, G)$.

Input 3 (Poitou–Tate). *Assume the three hypotheses of Setting 7.8. Let F be a number field, and if $\ell = 2$ let F have no real place. Then for every local datum $\mathscr{D}$ of F at ℓ, formed in an algebraic closure $\overline{F}$, and every integer h,*

$$\operatorname{len} Ш^1(\mathscr{D}, h) \;\leq\; \operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big).$$

LEAN 1 `Kum.dinfNil` · 2 `Tower.step0`; for $h \geq 1$ the statement is `Descends`, proved in `descends`, and the last sentence is `Descends.eq_twLen` · 3 `shaLeV`

On Input 1. Write $G = \mathrm{Gal}(\overline{L}/L)$. An element φ of $D_\infty(\ell, \ell, G)$ has order a power of ℓ, say ℓ^k, and is fixed by an open subgroup of G containing $\mathrm{Gal}_L(\overline{L}/L_\infty)$, hence by σ^{ℓ^n} for some n. As in the proof of Lemma 5.3(a), $(T-1)^{\ell^n} - (T^{\ell^n} - 1)$ is ℓ times a polynomial with integer coefficients, so $(\sigma - 1)^{\ell^n}\varphi$ is ℓ times an element of the module generated by the conjugates $\sigma^i\varphi$, each of which is again fixed by σ^{ℓ^n}; repeating this k times gives $(\sigma - 1)^{k\ell^n}\varphi = 0$.

On Input 2. Write $G = \mathrm{Gal}(\overline{L}/L)$ again. The length of a group of cohomology classes over the layer L_m is expressed through one operator on the module $X_\infty(\ell, \ell, G)$, which belongs to the top of the tower. The classes over L_m are first identified with the elements of $D_\infty(\ell, \ell, G)$ that are invariant under a twisted action of $\mathrm{Gal}_L(\overline{L}/L_m)$; this is the cohomological step. The invariants are the kernel of one operator on $D_\infty(\ell, \ell, G)$, and duality turns the kernel into a cokernel on $X_\infty(\ell, \ell, G)$. The proof is given in §8.

On Input 3. By the duality theorem of Poitou and Tate [NSW, VIII, §6], $Ш^1(\mathscr{D}, h)$ is dual to the corresponding subgroup of $H^2(\mathscr{D}, \mathbb{Z}_\ell(h+1))$; the coefficients are dual to each other: the homomorphisms from $\mathscr{Q}(\mathscr{D})(-h)$ to the group of the roots of unity of ℓ-power order form the module $\mathbb{Z}_\ell(h+1)$. In the archive the statement is deduced from the three hypotheses of Setting 7.8, which the cluster passes on unchanged.

Corollary 7.10 (unipotence on the Iwasawa module). *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$ and suppose that $X_\infty(\ell, \ell, G)$ is finitely generated. If $\sigma \in G$ satisfies $\kappa_\ell^{\overline{L}/L}(\sigma) \equiv 1 \pmod{\ell}$, that is, if $\sigma \in G_{\ell,1}$, then the action of σ on $X_\infty(\ell, \ell, G)$ is unipotent modulo ℓ.*

Proof. The element σ^{-1} satisfies the same congruence, so by Input 1 the operator $\sigma^{-1} - 1$ is locally nilpotent on $D_\infty(\ell, \ell, G)$. By the formula $(\sigma x)(\varphi) = x(\sigma^{-1}\varphi)$ of Definition 7.3, the action of σ on $X_\infty(\ell, \ell, G)$ is $g^\vee$, where g is the action of σ^{-1} on $D_\infty(\ell, \ell, G)$. Apply Proposition 7.9(d). □

LEAN `xUnip`, there for every $X_\infty(\ell, N, U)$ with U closed and normal and $\sigma \in U_{\ell,1}$ · the reformulation of the congruence `mem_levU_one`

Proposition 7.11 (Theorem D from one descending element). *In Setting 7.4, assume the three hypotheses of Setting 7.8, write $G = \mathrm{Gal}(\overline{L}/L)$, and suppose that the module $X_\infty(\ell, \ell, G)$ is generated by $R \geq 1$ elements. Let $\sigma \in G$ and an integer $a' \geq 0$ be such that*

(1) *the element $u = \kappa_\ell^{\overline{L}/L}(\sigma)$ of $\mathbb{Z}_\ell$ has level a';*
(2) *the field L contains a primitive root of unity of order $\ell^{a'}$;*
(3) *for all integers $h \geq 1$ and $m \geq 0$ and every number field L' that is a layer of index m over L for ℓ, $\operatorname{len} Ш^1_\ell(L', h) = \operatorname{len} \operatorname{cok}\big((u^h\sigma)^{\ell^m} - 1\big)$, where $u^h\sigma$ is the operator on $X_\infty(\ell, \ell, G)$ of Input 2.*

Then the tower bound of Definition 7.12 holds for (ℓ, R, L), with the field $K = \mathbb{Q}_\ell$, the exponent a' and R centres in $\mathbb{Z}_\ell$.

Proof of Proposition 7.11 and of Theorem D. For the proposition, the level a' is at least 1, so $u \equiv 1 \pmod{\ell}$. The module $X_\infty(\ell, \ell, G)$ is generated by R elements, so it is finitely generated, and by Corollary 7.10 the action γ of σ on it is unipotent modulo ℓ. So Setting 2.7 holds for $X = X_\infty(\ell, \ell, G)$, this pair (γ, u) and the level a'. The operator $u^h\sigma$ is $u^h\gamma$, so by (3) and Definition 2.6, $\operatorname{len} Ш^1_\ell(L', h) = \tau(\gamma, u; h, m)$ for $h \geq 1$ and every such layer L'. Theorem A gives centres $c_1, \dots, c_R \in \mathbb{Z}_\ell$ with

$$\operatorname{len} Ш^1_\ell(L', h) \;\leq\; R\big(\max\big(m, m_0(\ell, R)\big) + a' + B\big)$$

whenever $v_\ell(c_i - h) \leq B$ for all i, that is, $|c_i - h| \geq \ell^{-B}$. This is the first part of the tower bound, with $K = \mathbb{Q}_\ell$ and $R' = R$. For the second bound write $n = m_0(\ell, R)$, let L'' be a number field that is a layer of index n over L for ℓ, and let $\mathscr{D}$ be a local datum of L'' at ℓ. By Theorem B, $\operatorname{len} Ш^1_\ell(L', h) \leq \tau(\gamma, u; h, n) + R \cdot \max(m - n, 0)$. By (3) the term $\tau(\gamma, u; h, n)$ equals $\operatorname{len} Ш^1_\ell(L'', h)$, which is $\operatorname{len} Ш^1(\mathscr{D}, h)$ by Definition 7.7, and this is at most $\operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big)$ by Input 3 for the field $F = L''$, which is totally complex because it contains L.

For Theorem D write $a = a_\ell(L)$. By Lemma 8.6(c) there is $\sigma \in G$ that is a topological generator of G for the cyclotomic character of ℓ; then $u = \kappa_\ell^{\overline{L}/L}(\sigma)$ has level a, and L contains a primitive root of unity of order ℓ^a. By Input 2, condition (3) holds for the fields $L' = L_m$. A number field that is a layer of index m over L for ℓ is isomorphic to L_m over L (Lemma 8.6(b)), and the length depends on the field only up to isomorphism; so (3) holds for every layer. The proposition applies with $a' = a$: the tower bound holds for (ℓ, R, L), and for $L' = L_m$ and $L'' = L_n$ its two inequalities are (i) and (ii). □

LEAN `aBound_of_descends` · `aBound_of_isTower`

How the bound is used. Three steps lead from Theorem D to the window of the guide [Gu, §6]; they complete the cluster. The statements of this part are those of the archive, with their hypotheses. Only Corollary 7.14 is proved here; the others are not deformalized in this note, and the last one is stated without its objects, which belong to the guide.

Definition 7.12 (the tower bound). Let $R \geq 0$ be an integer and L a field. *The second bound holds for* (ℓ, R, L) if for all integers $h \geq 1$ and $m \geq 0$, every number field L' that is a layer of index m over L for ℓ, every number field L'' that is a layer of index $m_0(\ell, R)$ over L for ℓ, and every local datum $\mathscr{D}$ of L'' at ℓ,

$$\operatorname{len} Ш^1_\ell(L', h) \;\leq\; \operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big) + R \cdot \max\big(m - m_0(\ell, R), 0\big).$$

The tower bound holds for (ℓ, R, L) if the second bound holds for (ℓ, R, L) and there are a field K with an ultrametric absolute value that extends the ℓ-adic absolute value of $\mathbb{Q}_\ell$, integers $a' \geq 0$ and $0 \leq R' \leq R$, and elements $c_1, \dots, c_{R'} \in K$, such that L contains a primitive root of unity of order $\ell^{a'}$ and such that, for all integers $h \geq 1$ and $m, B \geq 0$ with $|c_i - h| \geq \ell^{-B}$ for all i, and every number field L' that is a layer of index m over L for ℓ,

$$\operatorname{len} Ш^1_\ell(L', h) \;\leq\; R'\left(\max\bigl(m, m_0(\ell, R)\bigr) + a' + B\right).$$

LEAN `Win.SecondBound` · `Win.ABound`

Definition 7.13 (the first bound). Let $R, a', Z \geq 0$ be integers, L a field and $\mathscr{E}$ a finite set of non-negative integers. *The first bound holds for* (ℓ, R, a', L) *up to* Z *outside* $\mathscr{E}$ if $\mathscr{E}$ has at most R elements and, for all integers h with $1 \leq h \leq Z$ that are not in $\mathscr{E}$, all integers $m \geq 0$ and every number field L' that is a layer of index m over L for ℓ,

$$\operatorname{len} Ш^1_\ell(L', h) \;\leq\; R\left(\max\bigl(m, m_0(\ell, R)\bigr) + a' + \lfloor \log_\ell Z \rfloor\right),$$

where $\lfloor \log_\ell Z \rfloor$ is read as 0 for $Z = 0$.

LEAN `Win.FirstBound`

Corollary 7.14 (exceptional twists in the tower). *Let $R \geq 0$ be an integer and L a field such that the tower bound holds for (ℓ, R, L). Then there is an integer $a' \geq 0$ such that L contains a primitive root of unity of order $\ell^{a'}$ and such that for every integer $Z \geq 0$ there is a finite set $\mathscr{E}$ of non-negative integers for which the first bound holds for (ℓ, R, a', L) up to Z outside $\mathscr{E}$.*

Proof. Take K, a', R' and the centres c_i of Definition 7.12, and let $\mathscr{E}$ be the set of the integers $1 \leq h \leq Z$ with $|c_i - h| < \ell^{-\lfloor \log_\ell Z \rfloor}$ for some i. By Lemma 6.1 each centre contributes at most one element, so $\mathscr{E}$ has at most $R' \leq R$ elements. For $1 \leq h \leq Z$ outside $\mathscr{E}$ the tower bound applies with $B = \lfloor \log_\ell Z \rfloor$, and $R' \leq R$. □

LEAN `Win.exc`

By Theorem D the hypothesis of Corollary 7.14 holds for the field L of Setting 7.4, and the corollary is then Corollary C for the lengths $\operatorname{len} Ш^1_\ell(L_m, h)$.

Finite generation. The hypothesis of Theorem D on the Iwasawa module is a condition on a finite group.

Lemma 7.15 (finite generation). *Let L be a number field with an algebraic closure $\overline{L}$, write $G = \mathrm{Gal}(\overline{L}/L)$, and let $R \geq 0$ be an integer. The following are equivalent.*

(a) *The field L is totally complex and contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$; $R \geq 1$; and the module $X_\infty(\ell, \ell, G)$ is generated by R elements.*

(b) *The field L contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$; $R \geq 1$; and $\operatorname{len} D_\infty(\ell, \ell, G)[\ell] \leq R$, where the left-hand side is the length of the submodule of the elements of $D_\infty(\ell, \ell, G)$ killed by ℓ.*

LEAN `Tower.isTower_iff`; the conditions in (a) are the hypotheses of Theorem D on (ℓ, L, R)

Theorem 7.16 (Ferrero and Washington, in the form of the archive). *Let F be a number field that is Galois over $\mathbb{Q}$ with an abelian Galois group and that contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$. There is an integer $r \geq 0$ such that for every integer $n \geq 0$ and every number field F' over F that contains a primitive root of unity of order ℓ^n and is generated over F by the roots of unity of order dividing ℓ^n, the quotient of the ideal class group of F' by the subgroup of the ℓ-th powers has at most ℓ^r elements.*

LEAN the statement `Published.FerreroWashington` · its proof in the archive `FW.ferreroWashington`

This is the theorem of Ferrero and Washington [FW] that the Iwasawa invariant μ of the cyclotomic $\mathbb{Z}_\ell$-extension of an abelian number field vanishes, in the equivalent form that the ℓ-rank of the class groups is bounded along the cyclotomic tower [Wa, Ch. 13]. The archive states it as a proposition and proves it; the statements that use it take it as a hypothesis. From it the archive deduces a bound for the length in Lemma 7.15(b), with one R for all the fields isomorphic to a given abelian field:

Proposition 7.17 (one R for an abelian field). *Assume the statement of Theorem 7.16. Let $\ell \neq 2$, let $q \geq 1$ be an integer divisible by ℓ, and let Δ be a subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$, the Galois group of the field of the q-th roots of unity over $\mathbb{Q}$, all of whose elements are congruent to 1 modulo ℓ. There is an integer $R \geq 0$ such that for every number field L isomorphic to the subfield fixed by Δ, with an algebraic closure $\overline{L}$ and $G = \mathrm{Gal}(\overline{L}/L)$, the module $X_\infty(\ell, 1, G)$ is generated by R elements and the conditions of Lemma 7.15(a) hold for (ℓ, L, R).*

LEAN `Two.towerFixed`

Proposition 7.18 (the tower bound for the fields of the guide). *Assume the statement of Theorem 7.16. Assume also that the conclusion of Theorem D holds without further hypotheses: for every prime number in the place of ℓ, every number field L and every integer R such that the conditions of Lemma 7.15(a) hold, the tower bound holds for the prime, R and L.*

(a) *Let $\ell \neq 2$, and let q and Δ be as in Proposition 7.17. For every number field L isomorphic to the subfield fixed by Δ there is an integer R such that the tower bound holds for (ℓ, R, L).*

(b) *For every integer $q \geq 1$ and every subgroup Δ of $(\mathbb{Z}/q\mathbb{Z})^\times$ there is an integer R such that, for all prime numbers $p \equiv 3 \pmod 8$ and $p' \equiv 7 \pmod{16}$ that do not divide q, there is a number field L for which the tower bound holds for $(2, R, L)$ and which is a base field of the tower for the prime 2 in the sense of the guide, for q, Δ, p and p'. This last condition ties L to the fields of §6 of the guide; it is not deformalized here.*

LEAN (a) `Two.fixedIn` · (b) `Two.twoIn`

The reference layer. For the second cohomology group in Theorem D (ii) the cluster takes as an input that it is finite, with a bound for its order in terms of the twist, the degree and the discriminant of the field:

Definition 7.19 (the cohomology bound). Let C be a real number. *The cohomology bound holds with the constant C* if for every prime number, written ℓ again, every totally complex number field L that contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$, every local datum $\mathscr{D}$ of L at ℓ and every integer $h \geq 1$, the group $H^2(\mathscr{D}, \mathbb{Z}_\ell(h+1))$ is finite and

$$\log \#H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big) \;\leq\; \exp\Big(\big(2h\,[L : \mathbb{Q}]\big)^C \log\big(2\,|d_L|\big)\Big),$$

where $\#$ is the number of elements, $[L : \mathbb{Q}]$ the degree and d_L the discriminant of L.

LEAN `LemmaK`

So all the lengths in Theorem D are finite, also at a centre, and the exceptional twists cost a bounded amount.

The window. By Corollary 7.14, for each of finitely many primes ℓ there are at most R_ℓ exceptional twists up to Z, where R_ℓ is the number of generators for ℓ. Their union has at

most $\sum_\ell R_\ell$ elements, whatever Z. An exceptional twist spoils the estimate only on one interval of scales, and an interval lemma finds a range of scales that avoids all of them:

Lemma 7.20 (a window). *Let $R \geq 0$ be an integer, let θ and Θ be real numbers with $0 < \theta \leq \Theta$, let $\Xi > 1$ be a real number, and let $\mathscr{E}$ be a finite set of non-negative integers with at most R elements. Put $J = 2^{R+2}(\Theta/\theta)^R$. There is a real number Y with $\Xi^{1/J} \leq Y$ and $Y^2 \leq \Xi$ such that for every real number ω with $Y \leq \omega \leq Y^2$, every $h \in \mathscr{E}$ with $h \leq \omega^\Theta$ satisfies $h \leq \omega^\theta$.*

LEAN `Win.window`

Proposition 7.21 (the window of the guide). (a) *Suppose that the cohomology bound of Definition 7.19 holds with some constant C, and that the conclusions (a) and (b) of Proposition 7.18 hold, the first for every odd prime in the place of ℓ. Then the statement of the window of the guide [Gu, §6] holds: there are constants, namely an integer for every pair (q, Δ), an integer for every prime and every pair (q, Δ), and a positive real number, such that for every real number $\Theta \geq 1$ the two families of bounds of the guide hold, with these constants, on a window of scales.*

(b) *Assume the three hypotheses of Setting 7.8 and the statement of Theorem 7.16, and suppose that the cohomology bound of Definition 7.19 holds with some constant C. Then the conclusion of (a) holds.*

LEAN (a) `Win.thmBab_of` · (b) `Win.thmBab_of_lemmaK`

The statement of the window is not deformalized in this note: its fields and its two families of bounds are the subject of §6 of the guide. Part (b) follows from part (a), Theorem D and Proposition 7.18.

Remark 7.22 (the classical picture). Let X be a module that is free of rank R, let $\gamma \in \mathrm{End}(X)$ and let u be a unit of $\mathbb{Z}_\ell$, and let $\Phi(T) = \det(T - (\gamma - 1))$ be the characteristic polynomial of $\gamma - 1$. Factoring $(u^h\gamma)^{\ell^m} - 1$ over the roots of unity gives

$$\tau(\gamma, u; h, m) = \sum_{\zeta^{\ell^m}=1} v_\ell\big(\Phi(\zeta u^{-h} - 1)\big).$$

At the layer 0 this reads $\tau(\gamma, u; h, 0) = v_\ell(\Phi(u^{-h} - 1))$: the twists with a large length are the integers close to a zero in $\mathbb{Z}_\ell$ of the function $s \mapsto \Phi(u^{-s} - 1)$. For the modules of this section, Φ is the characteristic polynomial of Iwasawa's theory [Iw], [Wa, Ch. 13], and for abelian fields and odd ℓ the main conjecture, proved by Mazur and Wiles [MW], expresses the characteristic polynomials of closely related modules through ℓ-adic L-functions. In this language an exceptional twist is, roughly, an integer that is ℓ-adically very close to a zero of an ℓ-adic L-function. None of this is used in the archive: the centres there come from a compactness argument, and only their number matters.

8 Descent to a layer

This section proves Input 2. The cohomological part of the proof is one isomorphism, which the archive proves in the neighbouring directory on towers of number fields. It is stated below as Input 2a, with a companion, Input 2b. Everything else is proved here: duality for modules over $\mathbb{Z}_\ell$, the group of principal units, and the Galois theory of the tower.

Characters. For a module M put $M^\vee = \mathrm{Hom}_{\mathbb{Z}_\ell}(M, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$, the module of *characters* of M. Thus $X = D^\vee$ in Proposition 7.9, and $X_\infty(\ell, N, U) = D_\infty(\ell, N, U)^\vee$ in Definition 7.3. By Proposition 7.9(a) the module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is injective: a homomorphism from a submodule of M to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ extends to a character of M.

Lemma 8.1. *Let M be a module over $\mathbb{Z}_\ell$ and W a submodule of M, and form the modules of characters with values in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$.*

(a) *For every non-zero $x \in M$ there is a character χ of M with $\chi(x) \neq 0$.*

(b) *The restriction map $M^\vee \to W^\vee$ is surjective. Its kernel is the image of the injective map $(M/W)^\vee \to M^\vee$ given by composition with the quotient map $M \to M/W$.*

(c) $\operatorname{len} M^\vee = \operatorname{len} M$.

Proof. (a) The elements $t \in \mathbb{Z}_\ell$ with $tx = 0$ form an ideal other than $\mathbb{Z}_\ell$, so this ideal is 0 or $\ell^k\mathbb{Z}_\ell$ with $k \geq 1$. Let y be the class of ℓ^{-k} in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, and the class of ℓ^{-1} if the ideal is 0. Then $y \neq 0$, and $ty = 0$ whenever $tx = 0$. So $tx \mapsto ty$ is a well-defined homomorphism from the submodule $\mathbb{Z}_\ell x$ to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, and a character χ that extends it has $\chi(x) = y$.

(b) Restriction is surjective because $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is injective. A character of M vanishes on W if and only if it factors through M/W, and then it does so in exactly one way.

(c) Let M have finite length n. We use induction on n; for $n = 0$ both modules are zero. Let $n \geq 1$. A composition series of M gives a submodule W of length $n-1$ such that M/W is simple. A simple module over $\mathbb{Z}_\ell$ is isomorphic to $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$, so its characters correspond, by their value at the class of 1, to the elements of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ killed by ℓ. These form the group $\ell^{-1}\mathbb{Z}_\ell/\mathbb{Z}_\ell$, which has length 1. By (b) and the induction hypothesis, $\operatorname{len} M^\vee = \operatorname{len}(M/W)^\vee + \operatorname{len} W^\vee = 1 + (n-1)$.

Now let M be any module. For a submodule W let $W^\perp \subseteq M^\vee$ be the submodule of the characters that vanish on W. If $W \subsetneq W'$ are submodules of M, then $W'^\perp \subsetneq W^\perp$: by (a) the module M/W has a character that does not vanish on the image of W', and its composition with $M \to M/W$ lies in $W^\perp$ and not in $W'^\perp$. So a chain of submodules of M gives a chain of the same length in $M^\vee$, and $\operatorname{len} M \leq \operatorname{len} M^\vee$. If the length of M is infinite, so is the length of $M^\vee$. □

LEAN (a) `Tower.qzSep`, with `exists_qz_ne_zero_annihilators_of_ne_zero` · (b) `exact_dual` · (c) `Tower.lenDual`, with `simple_dual` and `le_dual`

Lemma 8.2 (kernel and cokernel). *Let D be a module over $\mathbb{Z}_\ell$, let $g \in \mathrm{End}(D)$, and let $g^\vee$ be the endomorphism of $X = D^\vee$ given by $(g^\vee x)(\varphi) = x(g\varphi)$, as in Proposition 7.9. The image of $g^\vee$ consists of the characters of D that vanish on the kernel $\ker g$ of g, the restriction of characters to any submodule of D is surjective, and*

$$\operatorname{len} \operatorname{cok} g^\vee = \operatorname{len} \ker g.$$

Proof. A character of the form $g^\vee x = x \circ g$ vanishes on $\ker g$. Conversely, let $y \in X$ vanish on $\ker g$. Then $g\varphi \mapsto y(\varphi)$ is a well-defined homomorphism $g(D) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$. It extends to some $x \in X$, and $y = g^\vee x$. So the image of $g^\vee$ is the kernel of the restriction map $X \to (\ker g)^\vee$, which is surjective by Lemma 8.1(b). Hence $\operatorname{cok} g^\vee$ is isomorphic to $(\ker g)^\vee$, and Lemma 8.1(c) gives the lengths. □

LEAN the image and the surjectivity `Tower.dualKer`, there for a homomorphism between two modules · the lengths `Tower.cokerDual`

Principal units. Recall from §7 the groups $U_\ell^{(0)} = \mathbb{Z}_\ell^\times$ and $U_\ell^{(n)} = 1 + \ell^n\mathbb{Z}_\ell$ for $n \geq 1$. An element of $\mathbb{Z}_\ell$ has level n (Definition 2.5) if and only if it lies in $U_\ell^{(n)}$ and not in $U_\ell^{(n+1)}$, where $n \geq 1$, and $n \geq 2$ if $\ell = 2$.

Lemma 8.3. *Let $a \geq 1$ be an integer, and $a \geq 2$ if $\ell = 2$.*

(a) *For $n \geq 1$ the index of $U_\ell^{(n)}$ in $\mathbb{Z}_\ell^\times$ is $\ell^{n-1}(\ell-1)$. For $m \geq 0$ the index of $U_\ell^{(a+m)}$ in $U_\ell^{(a)}$ is ℓ^m.*

(b) *If $u \in U_\ell^{(a)}$, then $v_\ell(u^{\ell^m} - 1) = v_\ell(u-1) + m$ for every integer $m \geq 0$. In particular, if u has level a, then u^{ℓ^m} has level $a+m$.*

(c) *An element u of $U_\ell^{(a)}$ generates $U_\ell^{(a)}$ topologically, that is, $U_\ell^{(a)}$ lies in the closure of the set of the powers of u, if and only if u does not lie in $U_\ell^{(a+1)}$; and then u has level a.*

Proof. (a) Reduction modulo ℓ^n is a surjective homomorphism from $\mathbb{Z}_\ell^\times$ onto the group of units of the ring $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$, which has $\ell^{n-1}(\ell-1)$ elements, and its kernel is $U_\ell^{(n)}$. The second index is the quotient of two of these numbers.

(b) If $u = 1$, both sides are infinite. Otherwise u has the level $v_\ell(u-1) \geq a$, and Lemma 4.1 gives $v_\ell(u^{\ell^m} - 1) = v_\ell(u-1) + m$.

(c) An element of $U_\ell^{(a)}$ that is not in $U_\ell^{(a+1)}$ has level a. If $u \in U_\ell^{(a+1)}$, all powers of u lie in the closed subgroup $U_\ell^{(a+1)}$, which does not contain the element $1 + \ell^a$ of $U_\ell^{(a)}$. Now let u have level a, and let $m \geq 0$. By Lemma 4.1 an integer n satisfies $u^n \in U_\ell^{(a+m)}$ if and only if ℓ^m divides n. So the powers $u^0, u^1, \ldots, u^{\ell^m-1}$ lie in different cosets of $U_\ell^{(a+m)}$ in $U_\ell^{(a)}$, and by (a) there are no other cosets. Thus every element of $U_\ell^{(a)}$ is congruent modulo ℓ^{a+m} to a power of u, for every m: it lies in the closure of the set of powers of u. □

LEAN `Tower.princGen` · (a) `pg_index` · (b) `pg_emult`, from `emultiplicity_pow_sub_one_odd` and `emultiplicity_pow_sub_one_sq` · (c) `pg_exists`, `princ_le_of_isClosed`

Layers. The groups of the layers are subgroups of the Galois group that the archive defines through the exponent of Definition 7.2.

Definition 8.4 (the group of a layer). Let L be a number field with an algebraic closure $\overline{L}$, and let $m \geq 0$ be an integer. In the notation of §7, and with $a = a_\ell(L)$,

$$\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m} = \mathrm{Gal}(\overline{L}/L)_{\ell,a+m} = \left\{\sigma \in \mathrm{Gal}(\overline{L}/L) \,:\, \kappa_\ell^{\overline{L}/L}(\sigma) \in U_\ell^{(a+m)}\right\}.$$

It is a function of the prime, the field, its closure and m.

LEAN `Tower.layU`

Lemma 8.5 (roots of unity). *Let L be a number field with an algebraic closure $\overline{L}$; the hypothesis of Setting 7.4 on the roots of unity is not assumed. Write $G = \mathrm{Gal}(\overline{L}/L)$, and for $n \geq 0$ let $\zeta_n \in \overline{L}$ be a root of unity of order ℓ^n.*

(a) *For an integer $n \geq 0$, the field L contains a primitive root of unity of order ℓ^n if and only if $n \leq a_\ell(L)$.*

(b) *Let $F \subseteq F'$ be subfields of $\overline{L}$ such that F' contains ζ_n and is generated over F by the roots of unity of order dividing ℓ^n. Then the elements of G that fix every element of F' are the elements σ of G that fix every element of F and satisfy $\kappa_\ell^{\overline{L}/L}(\sigma) \in U_\ell^{(n)}$. In particular $\mathrm{Gal}_L(\overline{L}/L(\zeta_n)) = G_{\ell,n}$, and $G_{\ell,n} = G$ if and only if $n \leq a_\ell(L)$.*

(c) *The field L contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$, if and only if $a_\ell(L) \geq 1$, and $a_\ell(L) \geq 2$ if $\ell = 2$.*

(d) *If L contains the ℓ-th roots of unity, and the fourth roots of unity if $\ell = 2$, then L is totally complex.*

(e) *Let $\ell = 2$. Then $\kappa_2^{\overline{L}/L}(\sigma) \equiv 1 \pmod 4$ for all $\sigma \in G$ if and only if L contains the fourth roots of unity.*

Proof. (a) A power of a primitive root of unity of order ℓ^n is one of order $\ell^{n'}$, for every $n' \leq n$; so the integers in question are those up to the largest one, which is $a_\ell(L)$ by Definition 7.2.

(b) An automorphism that fixes F fixes F' if and only if it fixes the roots of unity of order dividing ℓ^n. Since $\sigma(\zeta) = \zeta^u$ with $u = \kappa_\ell^{\overline{L}/L}(\sigma)$ for these roots, this happens if and only if $u \equiv 1 \pmod{\ell^n}$. The case $F = L$, $F' = L(\zeta_n)$ is the first formula. Finally $G_{\ell,n} = G$ means that ζ_n lies in L, and (a) applies.

(c) This is (a) for $n = 1$, and for $n = 2$ if $\ell = 2$.

(d) A real embedding of L would map a root of unity of order ℓ, or of order 4 if $\ell = 2$, to a real root of unity of the same order; but the real roots of unity are 1 and -1.

(e) By (b), the congruence for all σ says that $G_{2,2} = G$, that is, $2 \leq a_2(L)$; by (a) this means that L contains a root of unity of order 4. □

LEAN (a), the second part of (b), (c), (d), (e) `Tower.muQ`, where the condition of (e), or $\ell \neq 2$, is one notion · (b) `Kum.galOfCyc`

Lemma 8.6. *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$ and $a = a_\ell(L)$, and for $n \geq 0$ let $\zeta_n \in \overline{L}$ be a root of unity of order ℓ^n.*

(a) *$\kappa_\ell^{\overline{L}/L}(G) = U_\ell^{(a)}$, where $a \geq 1$, and $a \geq 2$ if $\ell = 2$. For every $m \geq 0$ the index of $\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$ in G is ℓ^m, the field L_m is $L(\zeta_{a+m})$, it is a layer of index m over L for ℓ (Definition 7.5), and $\mathrm{Gal}_L(\overline{L}/L_m) = \mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$.*

(b) *Let $L' \subseteq \overline{L}$ be an extension of L that contains ζ_k and is generated over L by the roots of unity of order dividing ℓ^k, for an integer $k \geq 0$, and put $m = \max(k - a, 0)$. Then $L' = L_m$, the degree of L' over L is ℓ^m, and $\mathrm{Gal}_L(\overline{L}/L') = \mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$. Consequently a subfield of $\overline{L}$ that is a layer of index m over L for ℓ is L_m, and a number field that is a layer of index m over L for ℓ is isomorphic to L_m over L.*

(c) *There is $\sigma \in G$ that is a topological generator of G for the cyclotomic character of ℓ (Definition 7.1), and L contains a primitive root of unity of order ℓ^a. For every such σ the element $\kappa_\ell^{\overline{L}/L}(\sigma)$ of $\mathbb{Z}_\ell$ has level a, the element σ lies in $G_{\ell,1}$, and for every $m \geq 0$ the element σ^{ℓ^m} is a topological generator of $\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$ for the cyclotomic character of ℓ.*

Proof. (a) By Lemma 8.5(a) the field L contains ζ_a and not ζ_{a+1}, and by Lemma 8.5(c) and Setting 7.4 the inequalities for a hold. Every element of G fixes ζ_a, so $\kappa_\ell^{\overline{L}/L}(G) \subseteq U_\ell^{(a)}$. Some $\sigma \in G$ moves ζ_{a+1}. Then $\kappa_\ell^{\overline{L}/L}(\sigma) \notin U_\ell^{(a+1)}$, so this element has level a, and by Lemma 8.3(c) the closure of the set of its powers contains $U_\ell^{(a)}$. The image $\kappa_\ell^{\overline{L}/L}(G)$ is compact, hence closed, and it contains these powers. So $\kappa_\ell^{\overline{L}/L}(G) = U_\ell^{(a)}$.

The cyclotomic character maps the cosets of $\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$ in G bijectively onto the cosets of $U_\ell^{(a+m)}$ in $U_\ell^{(a)}$, and there are ℓ^m of these by Lemma 8.3(a). By Lemma 8.5(b) this group is $\mathrm{Gal}_L(\overline{L}/L(\zeta_{a+m}))$, and by Galois theory its index in G is the degree of $L(\zeta_{a+m})$

over L. So $L(\zeta_{a+m})$ is a subfield of L_∞ of degree ℓ^m over L, and it is a layer of index m. It is the only subfield of this degree: such a subfield is the fixed field of the preimage, under the cyclotomic character, of a closed subgroup of index ℓ^m in $U_\ell^{(a)}$. The quotient by this subgroup has ℓ^m elements, so the subgroup contains u^{ℓ^m} for a topological generator u of $U_\ell^{(a)}$. Hence it contains $U_\ell^{(a+m)}$ by Lemma 8.3(b) and (c), and the two groups have the same index.

(b) We have $L' = L(\zeta_k)$. If $k \le a$, then $L' = L = L_0$ and $m = 0$. If $k \ge a$, then by (a) the field $L' = L_{k-a}$ has degree ℓ^{k-a} over L. The group is given by (a). If moreover L' has degree $\ell^{m'}$ over L for an integer m', then $m' = m$; and a number field that is a layer over L can be embedded into $\overline{L}$ over L.

(c) The element σ of the proof of (a) has $\kappa_\ell^{\overline{L}/L}(\sigma)$ of level a, so by Lemma 8.3(c) the closure of the set of the powers of this element contains $U_\ell^{(a)} = \kappa_\ell^{\overline{L}/L}(G)$: it is a topological generator. The root of unity ζ_a lies in L. Now let σ be any topological generator of G. The element $\kappa_\ell^{\overline{L}/L}(\sigma)$ of $U_\ell^{(a)}$ generates $U_\ell^{(a)}$ topologically, so it has level a by Lemma 8.3(c); as $a \ge 1$, the element σ lies in $G_{\ell,1}$. By Lemma 8.3(b), $\kappa_\ell^{\overline{L}/L}(\sigma^{\ell^m}) = \kappa_\ell^{\overline{L}/L}(\sigma)^{\ell^m}$ has level $a+m$. Hence $\sigma^{\ell^m} \in \mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$, and by Lemma 8.3(c), with $a+m$ in place of a, the closure of the set of the powers of its image contains $U_\ell^{(a+m)}$, which is the image of $\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$ by (a). □

LEAN (a) `Tower.cycRange`, `Tower.layerGen`, `Tower.layerUniq`, with `Base.galEmbTop` · (b) `lu_key`, `Tower.layerUniq` · (c) `Tower.layerGen`, `genLevel`

Twists. The actions of the Galois group on the two modules of Definition 7.3 are twisted by powers of the cyclotomic character.

Definition 8.7 (twisted modules). Let F be a number field with an algebraic closure $\overline{F}$, let $N \ge 0$ be an integer, U a normal subgroup of $\mathrm{Gal}(\overline{F}/F)$, V any subgroup of $\mathrm{Gal}(\overline{F}/F)$, and h an integer. Then

$$D_\infty(\ell, N, U)(-h) \qquad \text{and} \qquad X_\infty(\ell, N, U)(h)$$

are the modules $D_\infty(\ell, N, U)$ and $X_\infty(\ell, N, U)$ on which $\sigma \in \mathrm{Gal}(\overline{F}/F)$ acts as $\kappa_\ell^{\overline{F}/F}(\sigma)^{-h}\sigma$ and as $\kappa_\ell^{\overline{F}/F}(\sigma)^{h}\sigma$, respectively, and

$$D_\infty(\ell, N, U)(-h)^V$$

is the submodule of the elements of $D_\infty(\ell, N, U)(-h)$ that are fixed by this action of every element of V.

LEAN `Tower.dTw` · `Tower.xTw` · `Tower.ShaD`

Lemma 8.8 (the two twists are dual). *In the situation of Definition 8.7, with the normal subgroup U and the integers N and h, let $\sigma \in \mathrm{Gal}(\overline{F}/F)$, $x \in X_\infty(\ell, N, U)$ and $\varphi \in D_\infty(\ell, N, U)$, and put $u = \kappa_\ell^{\overline{F}/F}(\sigma)$. Then*

$$\big(u^h \sigma x\big)(\varphi) = x\big(u^h \sigma^{-1}\varphi\big),$$

and $u^h = \kappa_\ell^{\overline{F}/F}(\sigma^{-1})^{-h}$. In the notation of Proposition 7.9: the operator by which σ acts on $X_\infty(\ell, N, U)(h)$ is $g^\vee$, where g is the operator by which σ^{-1} acts on $D_\infty(\ell, N, U)(-h)$.

Proof. By Definition 7.3, $(\sigma x)(\varphi) = x(\sigma^{-1}\varphi)$, and x is $\mathbb{Z}_\ell$-linear. □

LEAN `Tower.xTw_apply_apply`

Input 2a (the classes over a layer). *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$. Let $h \neq 0$ be an integer, let F be a number field that is a finite extension of L contained in L_∞, and let $\mathscr{D}$ be a local datum of F at ℓ whose algebraic closure is $\overline{L}$. Then there is an isomorphism of $\mathbb{Z}_\ell$-modules from $Ш^1(\mathscr{D}, h)$ onto $D_\infty(\ell, \ell, G)(-h)^{\mathrm{Gal}_L(\overline{L}/F)}$, given by restricting classes to $\mathrm{Gal}_L(\overline{L}/L_\infty)$.*

Input 2b (invariants). *In Setting 7.4, write $G = \mathrm{Gal}(\overline{L}/L)$. Let V be a subgroup of G, and let $\eta \in G$ be a topological generator of V for the cyclotomic character of ℓ (Definition 7.1). Then for every integer h the module $D_\infty(\ell, \ell, G)(-h)^V$ is the kernel of $g - 1$, where g is the operator by which η^{-1} acts on $D_\infty(\ell, \ell, G)(-h)$; and it is also the kernel of the same expression formed with η.*

LEAN 2a `Tower.desc` · 2b `Tower.shaDGen`

Both are proved in the neighbouring directory of the archive, there for any integer N in the second slot of Input 2b and any closed normal subgroup in the third. We indicate the standard arguments; they are not deformalized here.

On Input 2a. Write $G = \mathrm{Gal}(\overline{L}/L)$. The group $\mathrm{Gal}(L_\infty/F)$ is isomorphic to $\mathbb{Z}_\ell$, and a topological generator of it acts on $\mathcal{Q}_\ell^{\overline{L}/F}(-h)$ by a scalar different from 1 when $h \neq 0$. So the cohomology of this group with these coefficients vanishes in degrees 1 and 2, and restriction identifies the classes over F with the homomorphisms $\mathrm{Gal}_L(\overline{L}/L_\infty) \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$ that are invariant under the twisted action of $\mathrm{Gal}_L(\overline{L}/F)$. The same holds place by place, so the local conditions correspond, and $Ш^1(\mathscr{D}, h)$ becomes the module of invariants in $D_\infty(\ell, \ell, G)(-h)$.

On Input 2b. With G, V and η as in the statement, an element of $D_\infty(\ell, \ell, G)$ has finite order and is fixed by an open subgroup of G, so it is fixed by the twisted action of $G_{\ell,n}$ when n is large. For such n every $\rho \in V$ is the product of a power of η and an element of $G_{\ell,n}$, because $\kappa_\ell^{\overline{L}/L}(\rho)$ is congruent modulo ℓ^n to a power of $\kappa_\ell^{\overline{L}/L}(\eta)$. Hence an element fixed by η is fixed by V; and it is fixed by η exactly when it is fixed by η^{-1}.

Proof of Input 2. Write $G = \mathrm{Gal}(\overline{L}/L)$. Let $h \neq 0$ and $m \geq 0$ be integers, put $\eta = \sigma^{\ell^m}$ and $V = \mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$. By Lemma 8.6(a) the field L_m lies in L_∞ and $\mathrm{Gal}_L(\overline{L}/L_m) = V$. Choose a local datum $\mathscr{D}$ of L_m at ℓ whose algebraic closure is $\overline{L}$. By Definition 7.7 and Input 2a for $F = L_m$,

$$\operatorname{len} Ш^1_\ell(L_m, h) = \operatorname{len} Ш^1(\mathscr{D}, h) = \operatorname{len} D_\infty(\ell, \ell, G)(-h)^V.$$

By Lemma 8.6(c) the element η is a topological generator of V for the cyclotomic character of ℓ. So Input 2b applies: the module on the right is the kernel of $g - 1$, where g is the operator by which η^{-1} acts on $D_\infty(\ell, \ell, G)(-h)$. By Lemma 8.8, $g^\vee$ is the operator by which η acts on $X_\infty(\ell, \ell, G)(h)$, that is, $\kappa_\ell^{\overline{L}/L}(\eta)^h \eta$. Now $\kappa_\ell^{\overline{L}/L}(\eta) = u^{\ell^m}$, and the scalar u^h commutes with σ, so

$$g^\vee = u^{\ell^m h} \sigma^{\ell^m} = (u^h \sigma)^{\ell^m}.$$

Since $(g-1)^\vee = g^\vee - 1$, Lemma 8.2 gives

$$\operatorname{len} \operatorname{cok}\big((u^h\sigma)^{\ell^m} - 1\big) = \operatorname{len} \ker(g-1) = \operatorname{len} Ш^1_\ell(L_m, h).$$

For $h \geq 1$ the operator $u^h\sigma$ on $X_\infty(\ell, \ell, G)$ is $u^h\gamma$, so the left-hand side is $\tau(\gamma, u; h, m)$ by Definition 2.6. □

LEAN `Tower.step0` · `descends` · `Descends.eq_twLen`

The hypothesis $h \neq 0$ enters through Input 2a only. In the archive a layer is not a subfield of a fixed algebraic closure: it is any number field over L that is a layer in the sense of Definition 7.5. The formal proof begins by embedding such a field into $\overline{L}$, and Lemma 8.6(b) shows that the image is L_m.

9 Two examples

Both examples have $\ell = 3$ and $u = 4$, which has level $a = 1$; the special values stand in the slots of the notation, so the twisted length is $\tau(\gamma, 4; h, m)$ and the valuation is $v_3(\cdot)$. The modules are free, so the lengths are valuations of determinants (Lemma 3.2); the build script of this note computes them in exact rational arithmetic from the matrices and compares them with the formulas below.

Example 9.1 (two centres). Let $X = \mathbb{Z}_3^2$ and

$$\gamma = \begin{pmatrix} 4^{-5} & 1 \\ 0 & -2 \end{pmatrix}, \qquad \gamma \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 3,$$

so γ is unipotent modulo 3 and $R = 2$; the reference layer is $m_0(3, 2) = 3$. The eigenvalues are 4^{-5} and -2, and $(-2)^2 = 4$. The operator $(u^h\gamma)^{3^m} - 1$ is triangular, with diagonal entries $4^{3^m(h-5)} - 1$ and $z - 1$, where $z = (-2 \cdot 4^h)^{3^m}$. Since $z \equiv 1 \pmod 3$, the numbers $z - 1$ and $z^2 - 1 = 4^{3^m(2h+1)} - 1$ have the same valuation. By Lemma 4.1,

$$\tau(\gamma, 4; h, m) = 2\,(m + 1) + v_3(5 - h) + v_3\!\left(-\tfrac{1}{2} - h\right) \qquad (h \neq 5), \qquad \tau(\gamma, 4; 5, m) = \infty.$$

The centres are $c_1 = 5$ and $c_2 = -\frac{1}{2}$, and Theorem A is an equality for $m \geq m_0(3, 2)$. The first centre is an integer: at $h = 5$ the operator $(u^h\gamma)^{3^m} - 1$ is singular and the cokernel is infinite. The second is not an integer, and the integers $1, 4, 13, 40, 121, \ldots$ approach it. For $Z = 150$ we have $\lfloor \log_\ell Z \rfloor = 4$, and the exceptional twists are 5 and 121. Every other twist up to 150 has $v_3(c_1 - h) + v_3(c_2 - h) \leq 4$. The formula was confirmed for all $1 \leq h \leq 150$ and the 5 layers $0 \leq m < 5$.

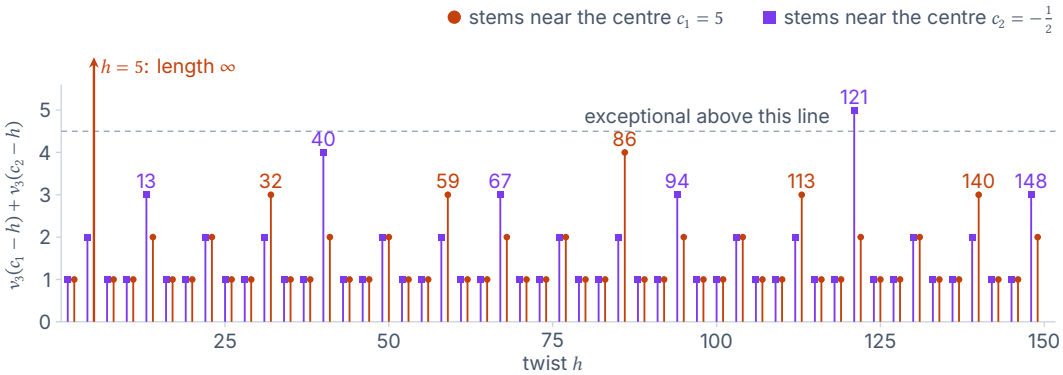


Figure. Example 9.1: the part of the length that depends on the twist. Each stem belongs to one centre; a label is the twist. The two stems that pass the dashed line are the exceptional twists for $Z = 150$.

Example 9.2 (why a reference layer). Let $X = \mathbb{Z}_3^3$ and let γ permute the coordinates cyclically. Then $\gamma^3 = 1$, so $(\gamma - 1)^3 \equiv 0 \pmod 3$ and γ is unipotent modulo 3; here $R = 3$. Since $\det(t\gamma - 1) = t^3 - 1$, Lemma 4.1 gives $\tau(\gamma, 4; h, 0) = 2 + v_3(h)$, while $(u^h\gamma)^{3^m}$ is the scalar $u^{3^m h}$ for $m \geq 1$, so $\tau(\gamma, 4; h, m) = 3\,(1 + m + v_3(h))$.

layer m	0	1	2	3	4
$\tau(\gamma, 4; 1, m)$	2	6	9	12	15
$\tau(\gamma, 4; 9, m)$	4	12	15	18	21

From the layer 1 on, each step costs exactly $R = 3$: Theorem B is sharp. The step from the layer 0 to the layer 1 costs 8 at $h = 9$, more than R. Lemma 5.4 does not apply there, because $u^h\gamma$ is not congruent to 1 modulo 9. A reference layer is needed, and Proposition 5.5 shows that it can be taken to depend on ℓ and R alone.

Modules with torsion. The two examples are free modules. As a test of Proposition 5.5 where determinants are not available, the script also draws 120 random modules, for $\ell = 2, 3, 5$, each the sum of a free module of rank at least 1 and a non-zero finite module, with a random endomorphism that is unipotent modulo ℓ and a random twist, and computes the lengths from invariant factors. In all 360 steps between consecutive layers, starting at the layer $\lfloor \log_\ell R \rfloor + 2$, the length grew by at most R.

10 Notes on the formal text

Reading the Lean text for the mathematics, and not only for its statements, brought out the following points.

1. *No logarithm, no structure theorem.* A textbook proof would take the ℓ-adic logarithm of the eigenvalues, or the structure theorem for modules over the Iwasawa algebra, and would have to treat eigenvalues that are not principal units, as well as torsion. The formal proof replaces all of this by the ultrametric inequality of Lemma 4.2 and the compactness of $\mathbb{Z}_\ell$. The centres are not computed and are not canonical: they depend on the presentation, on the lift S, and on a choice in a non-empty intersection of balls.
2. *The reference layer has one layer to spare.* The formal proof of Proposition 5.5 proves the step for all $n \geq \lfloor \log_\ell R \rfloor + 2$ and applies it from $m_0(\ell, R)$ on, and the centres can be taken at any layer. So Theorems A, B and D hold with $\lfloor \log_\ell R \rfloor + 2$ in place of $m_0(\ell, R)$. This sharper form is not in the archive; the random test of §9 starts at that layer. The archive's value is kept in the statements above.
3. *Unipotence is needed for growth only.* Corollary 4.7 holds for every endomorphism.
4. *The formal statement is weaker than its proof.* The archive's form of Theorem D (i) asserts only that there exist a field with an ultrametric norm extending that of $\mathbb{Q}_\ell$, centres in it, at most R in number, and an exponent in place of a for which L contains the roots of unity of that order; this is the tower bound of Definition 7.12, and it is stated for every layer in the sense of Definition 7.5. Its proof gives centres in $\mathbb{Z}_\ell$, exactly R of them, and the exponent a; this is the form stated in Theorem D (i). The extra generality is carried through Corollary 7.14 and is used nowhere else.
5. *Infinite lengths are part of the statement.* Lengths take values in $\{0, 1, \dots, \infty\}$, and Theorem A holds at a singular twist only because both sides are infinite. Finiteness at every twist is a consequence of Theorem D (ii) and of the finiteness of the group H^2, not of the algebra.
6. *Where the hypotheses on the field enter.* The roots of unity in L make the image of the cyclotomic character of $\mathrm{Gal}(\overline{L}/L)$ procyclic and give the level of u. They also make L totally complex (Lemma 8.5(d)), which Input 3 needs when $\ell = 2$; the archive lists

this as a separate hypothesis of Theorem D and proves elsewhere that it is implied (Lemma 7.15). That lemma is not used by the five final theorems: none of them reaches it in the graph of dependencies of the archive.

7. *The exponent is lifted twice.* Lemma 4.1 rests in the archive on a statement about discrete valuation rings, which has its own proof in a directory on local rings. Lemma 8.3(b) rests there on two formulas for the multiplicity of ℓ in $u^n - 1$, one for odd ℓ and one for $u \equiv 1 \pmod{\ell^2}$, which a directory on bounds for class numbers deduces from the corresponding statement of the Lean library Mathlib. Neither refers to the other. Here both are Lemma 4.1.

8. *What is proved about descent, and where.* The formal proof of Input 2 belongs to the same unit of the archive as the algebra of this note (Appendix A), and §8 follows it. The step that is cohomology, Input 2a, and Input 2b lie outside this unit. Input 2b is stated for every integer h, Input 2a and Input 2 for $h \neq 0$; Theorem D uses $h \geq 1$.

Some proofs above differ from the formal ones. The archive proves Lemma 5.3(c) by an explicit computation with elements, where the ideals I_n are used here, and states Lemma 5.3(a) as an equivalence: one side is congruent to 0 if and only if the other is. Lemma 4.5 is proved there through the characteristic polynomial, and Lemma 4.1 for a general discrete valuation ring. In Lemma 8.1(c) the archive shows that the characters of a simple module are the multiples of one of them, where the isomorphism with $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$ is used here. It proves Lemma 8.3(c) from a statement of another directory: a closed subgroup of $\mathbb{Z}_\ell^\times$ that contains an element of level a contains $U_\ell^{(a)}$. The uniqueness of L_m as a subfield of L_∞, in the proof of Lemma 8.6(a), is not in the archive, where a layer is defined as in Definition 7.5. The short proofs of Lemma 8.5, of Lemma 8.8 and of Corollary 7.14 are written for this note from the definitions; they were not compared with the formal proofs step by step. In all other places the proofs follow the formal text step by step.

For §8 the formal proofs were not read in the Lean text itself. They were read in the structured proofs of the reading project, in which every step quotes the lines of the archive that it renders. A program compared the quotations with the archive, for all 452 steps of the 58 proofs of the unit, and found that no line of these proofs is left without a step. The statements of §8 were compared with the Lean text, as everywhere in this note.

Changes in this edition. Earlier editions wrote the twisted length as a function of the twist and the layer alone, and stated the hypotheses of Theorems A to D in sentences before the statements. That hid the endomorphism and the scalar for which the centres are chosen, and with them the assumption on the endomorphism. In this edition every function that the archive defines is written with all the arguments of its formal definition, in every place, and every theorem cites the Setting that holds its hypotheses.

Beyond the twisted length, the reference layer and the valuation, this changes the arithmetic part. The two modules of §7, written without arguments before, are $D_\infty(\ell, N, U)$ and $X_\infty(\ell, N, U)$, with $N = \ell$ and the whole Galois group in the slots for the modules of Theorem D. The exponent that was a is $a_\ell(L)$. The groups of principal units and their preimages in the Galois group, which carried one index before, are $U_\ell^{(n)}$ and $\mathrm{Gal}(\overline{L}/L)_{\ell,n}$, the group of a layer is $\mathrm{Gal}(\overline{L}/L)_{\ell,\, a_\ell(L)+m}$, and the Galois group is written with the field and its closure. The cyclotomic character carries the prime, the field and the closure, and so do the Tate twists. The twisted module and its invariants carry all their arguments. The

length of the classes is $\operatorname{len} Ш^1_\ell(F,h)$, and the length of the second cohomology group is $\operatorname{len} H^2\big(\mathscr{D},\mathbb{Z}_\ell(h+1)\big)$, a function of a local datum, which earlier editions did not name.

The definitions that stood in running text (the valuation, generators, cokernels and congruences in §2; the objects of §7 and §8) are now definitions of their own. The three hypotheses on Galois cohomology, which earlier editions named in a paragraph after Theorem D, are Setting 7.8, and Theorem D and Input 3 assume them in their statements. Theorem D (ii) is stated for every local datum, and the theorem ends with the form of its conclusion that the archive states (Definition 7.12). The statements of the last part of §7, which earlier editions described in three paragraphs, are stated with their hypotheses. Lemma 5.1(b), Lemma 6.1 and Lemma 8.3(b) are stated in the generality of the archive; Lemma 3.1(c), Lemma 5.4, Proposition 7.9, Lemma 8.5, Lemma 8.8, Corollary 7.10 and Proposition 7.11 state, as parts or as statements of their own, what earlier editions said inside proofs or between the statements; and Corollary 7.14 is the form of Corollary C that the archive proves.

Theorems A and B, Corollary C, the bounds of Theorem D and the inputs say what they said before, and the arguments of the proofs are the same; some of them moved with the statements they prove.

Appendix A. Concordance with the Lean archive

Each name is a link to the lines of the declaration at commit `40e56bab` of the public mirror of the archive. The line ranges and the quotations below are read from the archive by the build script, which also checks them against the SHA-256 of each file. The reading project divides the part of the archive that the final theorems use into units. This note is the note of one unit: the 51 declarations of the directory that the final theorems use, and 16 declarations of the neighbouring directory on towers of number fields, those that prove Input 2. The table contains all 67 of them, and the build of the note fails if one is missing.

In this note	Lean declaration	File	Lines
Def. 2.2	`GenBy`	CokLenLeOfRangeLe.lean	9–10
Def. 2.6	`jZero`	CokLenLeOfRangeLe.lean	12–12
Def. 2.5	`IsLevel`	CokLenLeOfRangeLe.lean	16–16
Def. 2.3	`cokLen`	CokLenLeOfRangeLe.lean	20–20
Def. 2.3	`InPow`	CokLenLeOfRangeLe.lean	22–22
Def. 2.4	`Unip`	CokLenLeOfRangeLe.lean	24–24
Def. 2.6	`twLen`	CokLenLeOfRangeLe.lean	26–26
Lemma 3.1(a)	`cokLen_le_of_range_le`	CokLenLeOfRangeLe.lean	28–30
Lemma 3.1(b)	`Base.lenComp`	LenComp.lean	17–41
Lemma 3.2	`length_cokernel_eq_addVal_det`	LengthDet.lean	52–68
Prop. 3.3	`lift`	ImportsAlt.lean	7–44
Lemma 4.1	`abelian₂.lte`	IsUnitAddMem.lean	109–126
Lemma 4.1	`lteNorm`	LteNorm.lean	19–94
Lemma 4.2	`padic_units_distance_le_max`	PadicUnitsDistanceLeMax.lean	8–35
Lemma 4.3	`helly`	Helly.lean	6–25
Prop. 4.4	`ball`	PadicUnitsDistanceLeMax.lean	37–63
Lemma 4.5	`detFactor`	DetFactor.lean	6–49
Prop. 4.6, proof	`normVal`	NormVal.lean	30–46
Prop. 4.6	`detBound`	DetBound.lean	9–34
Cor. 4.7	`exists_centres_level`	ExistsCentresLevel.lean	23–32
Lemma 5.1(a)	`cokL`	CokLen.lean	6–41
Lemma 5.1(b)	`nilLen`	NilLen.lean	29–59

In this note	Lean declaration	File	Lines
Lemma 5.2(a)	`unipPow`	UnipPow.lean	8–46
Lemma 5.3(a)	`frob`	Imports.lean	6–36
Lemma 5.3(b), (c)	`powIn`	PowIn.lean	6–29
Lemma 5.4	`phi`	ImportsTer.lean	7–46
Lemma 5.4	`step`	ImportsMore.lean	9–22
Lemma 3.1(c)	`mono`	ImportsBis.lean	6–13
Lemma 5.2(b)	`twist`	ImportsFurther.lean	7–50
Prop. 5.5	`growth`	Growth.lean	11–56
Theorem B	`twLen_le_growth`	ExistsCentresLevel.lean	17–21
Theorem A	`exists_centres`	ExistsCentresLevel.lean	34–49
Cor. C, the bound	`exists_centres_norm`	ExistsCentresLevel.lean	57–69
Lemma 6.1	`Win.near1`	Near1.lean	6–43
Cor. 7.14	`Win.exc`	Exc.lean	7–42
Prop. 7.9(a)	`qzInj`	QzInj.lean	8–27
Prop. 7.9(c)	`dualDiv`	DualDiv.lean	8–31
Prop. 7.9(b)	`torsFin`	TorsFin.lean	9–84
Prop. 7.9(d)	`dualUnip`	DualUnip.lean	9–34
Def. 7.3	`XDual`	Mk0IdMapCongr.lean	90–99
Theorem D	`Tower.IsTower`	XTwApplyApply.lean	120–124
Def. 7.5	`IsLayer`	StmtFields.lean	47–48
Def. 7.6	`shaInv`	LevelInertiaLeLevelDec.lean	70–71
Def. 7.7	`VLen`	Statement.lean	80–80
Def. 7.12	`Win.ABound`	SecondBound.lean	19–25
Def. 7.12	`Win.SecondBound`	SecondBound.lean	13–17
Def. 7.13	`Win.FirstBound`	SecondBound.lean	27–30
Input 1	`Kum.dinfNil`	DinfNil.lean	62–235
Cor. 7.10	`xUnip`	XUnip.lean	9–27
Input 2	`Tower.step0`	ExistsDescends.lean	26–46
Lemma 7.15	`Tower.isTower_iff`	ExistsDescends.lean	60–62
Input 2	`Descends`	ABoundOfDescends.lean	16–18
Input 2	`descends`	Descends.lean	8–15
Lemma 8.6(a)	`Tower.cycRange`	CycRange.lean	9–62
Lemma 8.6(c)	`genLevel`	GenLevel.lean	11–31
Input 3	`shaLeV`	ShaLeV.lean	7–16
Prop. 7.11	`aBound_of_descends`	ABoundOfDescends.lean	36–55
Theorem D	`aBound_of_isTower`	ABoundOfIsTower.lean	7–11
Theorem 7.16	`Published.FerreroWashington`	FerreroWashington.lean	7–11
Theorem 7.16	`FW.ferreroWashington`	FerreroWashington.lean	104–119
Prop. 7.17	`Two.towerFixed`	IsAlgClosureRat.lean	98–110
Prop. 7.18(a)	`Two.fixedIn`	IsAlgClosureRat.lean	139–141
Prop. 7.18(b)	`Two.twoIn`	IsAlgClosureRat.lean	133–137
Def. 7.19	`LemmaK`	LemmaK.lean	13–17
Lemma 7.20	`Win.window`	Window.lean	7–43
Prop. 7.21(a)	`Win.thmBab_of`	ThmBabOf.lean	11–103
Prop. 7.21(b)	`Win.thmBab_of_lemmaK`	ThmBabOfLemmaK.lean	9–12
Def. 2.1	`vl`	CokLenLeOfRangeLe.lean	14–14
Lemma 4.1, proof	`norm_le_of_dvd'`	LteNorm.lean	7–10
Lemma 4.1, proof	`norm_eq_of_addVal`	LteNorm.lean	12–17
Prop. 4.6, proof	`dvd_of_norm_le'`	NormVal.lean	6–19
Prop. 4.6, proof	`vl_prod`	NormVal.lean	21–28
Lemma 5.1(b), proof	`nilLen_range_succ`	NilLen.lean	6–9
Lemma 5.1(b), proof	`nilLen_lt`	NilLen.lean	11–27
Cor. C, the bound	`vl_le_of_norm`	ExistsCentresLevel.lean	51–55
Cor. 7.10	`mem_levU_one`	ABoundOfDescends.lean	22–28
Input 2	`Descends.eq_twLen`	ABoundOfDescends.lean	30–34

In this note	Lean declaration	File	Lines
Lemma 8.1(a)	`Tower.qzSep`	QzSep.lean	47–66
Lemma 8.1(a), proof	`exists_qz_ne_zero_annihilators_of_ne_zero`	QzSep.lean	8–45
Lemma 8.1(b)	`exact_dual`	LenDual.lean	39–47
Lemma 8.1(c), proof	`simple_dual`	LenDual.lean	49–109
Lemma 8.1(c), proof	`le_dual`	LenDual.lean	10–37
Lemma 8.1(c)	`Tower.lenDual`	LenDual.lean	111–137
Lemma 8.2	`Tower.dualKer`	DualKer.lean	7–40
Lemma 8.2	`Tower.cokerDual`	CokerDual.lean	8–19
Lemma 8.3(a)	`pg_index`	PrincGen.lean	24–30
Lemma 8.3(c), proof	`pg_exists`	PrincGen.lean	32–47
Lemma 8.3(b)	`pg_emult`	PrincGen.lean	13–22
Lemma 8.3	`Tower.princGen`	PrincGen.lean	49–117
Lemma 8.3(c), proof	`princ_le_of_isClosed`	Generate.lean	103–109
Lemma 8.3(b), proof	`emultiplicity_pow_sub_one_odd`	EmultiplicityPowSubOneOdd.lean	46–52
Lemma 8.3(b), proof	`emultiplicity_pow_sub_one_sq`	EmultiplicityPowSubOneOdd.lean	72–88
Def. 7.2	`Tower.cZero`	XTwApplyApply.lean	104–104
Def. 8.4	`Tower.layU`	XTwApplyApply.lean	108–108
Lemma 8.5	`Tower.muQ`	CycMemPrincIff.lean	81–104
Lemma 8.5(b)	`Kum.galOfCyc`	GalOfCyc.lean	5–65
Lemma 8.6(a), proof	`Base.galEmbTop`	GalEmbTop.lean	32–69
Lemma 8.6(b)	`lu_key`	LayerUniq.lean	11–23
Lemma 8.6(a), (b)	`Tower.layerUniq`	LayerUniq.lean	25–43
Lemma 8.6(a), (c)	`Tower.layerGen`	LayerGen.lean	10–39
Def. 7.1	`Tower.IsGen`	XTwApplyApply.lean	36–37
Def. 8.7	`Tower.dTw`	XTwApplyApply.lean	56–56
Def. 8.7	`Tower.xTw`	XTwApplyApply.lean	58–58
Lemma 8.8	`Tower.xTw_apply_apply`	XTwApplyApply.lean	66–69
Def. 8.7	`Tower.ShaD`	XTwApplyApply.lean	73–74
Input 2a	`Tower.desc`	Imports.lean	10–147
Def. 7.7	`shaLen_eq_shaInv`	ShaLenEqShaInv.lean	58–60
Input 2b	`Tower.shaDGen`	ShaDGen.lean	9–59

Four statements as they are written in the archive. Theorem D:

```
theorem UpperTheory.V.PropA.aBound_of_isTower (hP : GlobalTheory.Published.PoitouTateDuality) (hF :
    LocalFinitenessK) (hT : LocalTateDualityK)
    (l : ℕ) [Fact l.Prime] (L₀ : Type) [Field L₀] [NumberField L₀] (R : ℕ) (ht : UpperTheory.V.Tower.IsTower l L₀
       R) :
    UpperTheory.V.Win.ABound l R L₀
```

Its conclusion, the tower bound of Definition 7.12, with the second bound; here `e` is the twist h, `s` the centres, `c` the exponent a', which the proof takes to be the level a, `jZero l R` the reference layer $m_0(\ell, R)$, `shaInv L₁ l e` the length $\operatorname{len} Ш^1_\ell(L', h)$ and `VLen D e` the length $\operatorname{len} H^2\big(\mathscr{D}, \mathbb{Z}_\ell(h+1)\big)$:

```
def ABound (l R : ℕ) [Fact l.Prime] (L₀ : Type) [Field L₀] : Prop :=
  (∃ (K : Type) (_ : NormedField K) (_ : NormedAlgebra ℚ_[l] K) (_ : IsUltrametricDist K) (c R' : ℕ) (s : Fin R'
     → K),
    R' ≤ R ∧ (∃ ζ : L₀, IsPrimitiveRoot ζ (l ^ c)) ∧
    ∀ e : ℕ, 1 ≤ e → ∀ (m : ℕ) (L₁ : Type) [Field L₁] [NumberField L₁] [Algebra L₀ L₁], IsLayer l m L₀ L₁ →
      ∀ B : ℕ, (∀ i, (l : ℝ) ^ (-(B : ℤ)) ≤ ‖s i - (e : K)‖) →
        shaInv L₁ l e ≤ ((R' * (max m (jZero l R) + c + B) : ℕ) : ℕ∞)) ∧
  SecondBound l R L₀

def SecondBound (l R : ℕ) [Fact l.Prime] (L₀ : Type) [Field L₀] : Prop :=
  ∀ e : ℕ, 1 ≤ e → ∀ (m : ℕ) (L₁ : Type) [Field L₁] [NumberField L₁] [Algebra L₀ L₁], IsLayer l m L₀ L₁ →
    ∀ (L₂ : Type) [Field L₂] [NumberField L₂] [Algebra L₀ L₂], IsLayer l (jZero l R) L₀ L₂ →
```

```
∀ (Ω : Type) [Field Ω] [Algebra L₂ Ω] [IsAlgClosure L₂ Ω] (D : LData L₂ Ω l),
  shaInv L₁ l e ≤ VLen D e + ((R * (m - jZero l R) : ℕ) : ℕ∞)
```

Theorem A, where `twLen γ u e m` is $\tau(\gamma, u; h, m)$, with all four arguments in the same order, and `vl l x` is the valuation $v_\ell(x)$. The endomorphism `γ` and the scalar `u` are bound, with their hypotheses, before the centres `s`:

```
theorem exists_centres {R c : ℕ} {γ : Module.End ℤ_[l] X} {u : ℤ_[l]} (hX : GenBy l R X) (hγ : Unip γ) (hu :
    IsLevel l u c) :
    ∃ s : Fin R → ℤ_[l], ∀ e m : ℕ,
      twLen γ u e m ≤ ∑ i, (((max m (jZero l R) + c : ℕ) : ℕ∞) + vl l (s i - e))
```

Input 2, where `γ` is the element σ of $G = \mathrm{Gal}(\overline{L}/L)$, `xTw l l T e γ` is the operator $u^h\sigma$ on $X_\infty(\ell, \ell, G)$, with the prime, $N = \ell$ and the whole group in its first three slots, `cokerLen` is the length of a cokernel, and `IsLayer l m L₀ L₁` says that `L₁` is a layer of index m over `L₀` for ℓ (Definition 7.5):

```
theorem step0 (hμ : HasMuQ l L₀) {γ : G L₀ Ω} (hγ : IsGen l T γ) {e : ℤ} (he : e ≠ 0) (m : ℕ) (L₁ : Type) [Field
    L₁]
    [NumberField L₁] [Algebra L₀ L₁] (hL : IsLayer l m L₀ L₁) :
    shaInv L₁ l e = cokerLen (xTw l l (T : Subgroup (G L₀ Ω)) e γ ^ l ^ m - 1)
```

Notation

The symbols of the text. A function that the archive defines is listed with all its arguments; the brackets give its formal name with its arguments, or the letter used in the archive.

ℓ, $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$, $\overline{\mathbb{Q}}_\ell$ a prime; the ℓ-adic integers and numbers; an algebraic closure

$v_\ell(x)$, $|z|$ ℓ-adic valuation of x, with $v_\ell(\ell) = 1$ [`vl l x`]; absolute value $\ell^{-v_\ell(z)}$

X, R, π a $\mathbb{Z}_\ell$-module; a number of generators; a surjection $\mathbb{Z}_\ell^R \to X$ [`GenBy l R X`]

$\operatorname{len} M$ length of a module M

$\mathrm{End}(X)$, $\operatorname{cok} f$, $\ker f$ endomorphisms; cokernel $X/f(X)$ [its length: `cokLen f`]; kernel

I_n, $f \equiv g \pmod{\ell^n}$ endomorphisms with image in $\ell^n X$; $f - g \in I_n$ [`InPow n (f - g)`]

γ an endomorphism of X, an argument of the twisted length

u, a an element of $\mathbb{Z}_\ell$, an argument of the twisted length; its level $v_\ell(u-1)$ [c; `IsLevel l u c`]

h, m twist [e]; layer

$m_0(\ell, R)$ reference layer $\lfloor \log_\ell R \rfloor + 3$ of the prime ℓ and the number R [`jZero l R`]

$\tau(\gamma, u; h, m)$ twisted length of the pair (γ, u) at twist h and layer m (Definition 2.6) [`twLen γ u e m`]

c, c_i a centre; the centres [s_i]

Z, $\mathscr{E}_Z$, $\mathscr{E}$, B range of twists; exceptional twists up to Z; a finite set of twists; a bound for $v_\ell(c_i - h)$

K, a', R' a field with an ultrametric absolute value extending that of $\mathbb{Q}_\ell$; an exponent and a number of centres (Definition 7.12)

f, g, w, ν endomorphisms; $\nu = 1 + w + \cdots + w^{\ell-1}$

A, P, Q, d_i a square matrix; invertible matrices; elementary divisors (Lemma 3.2)

S, t, t', z, z_i a matrix lifting an endomorphism; scalars; an element of $\overline{\mathbb{Q}}_\ell$; eigenvalues

n, n', i, j, k, r, m' integers: exponents, indices, layers

x, y, b_n, r_n elements of a module, of $\mathbb{Z}_\ell$ or of a field; points and radii (Lemma 4.3)

T an indeterminate

D, $D[\ell]$, φ, $g^\vee$ a module, its elements killed by ℓ, an element; the dual endomorphism

$M^\vee$, χ the characters $M \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$ of a module M (§8); a character

W, W', $W^\perp$ submodules; the characters that vanish on W

F, $\overline{F}$, F', L, $\overline{L}$, L', L'' number fields, algebraic closures of them, extensions

$\mathrm{Gal}(\overline{F}/F)$, G the Galois group, with the field and its closure [`G F Ω`]; inside a statement, a name for $\mathrm{Gal}(\overline{L}/L)$

$\kappa_\ell^{\overline{F}/F}(\sigma)$ the ℓ-adic cyclotomic character of $\mathrm{Gal}(\overline{F}/F)$ at σ [`cycZ F Ω l σ`]

σ, ρ, ρ', η, ζ, ζ_n elements of a Galois group; a root of unity, one of order ℓ^n

$U_\ell^{(n)}$ the units of $\mathbb{Z}_\ell$ congruent to 1 modulo ℓ^n [`princ l n`]

U, V, $U_{\ell,n}$, $U_{\ell,\infty}$ subgroups of a Galois group; the elements of U whose cyclotomic character lies in $U_\ell^{(n)}$ [`levU l U n`], or is 1 [`cycU l U`]

$a_\ell(L)$ the largest n with a primitive root of unity of order ℓ^n in L [`cZero l L`]

$\mathrm{Gal}(\overline{L}/L)_{\ell, a_\ell(L)+m}$ the group of the layer m (Definition 8.4) [`layU l L Ω m`]

L_m, L_∞ the layers of the cyclotomic tower of Setting 7.4; their union

$\mathcal{O}$, $\mathfrak{p}$, $F_\mathfrak{p}$ a valuation ring of $\overline{F}$; a prime of F; the completion

N, Λ, $D_N(U;\Lambda,M)$ an integer, a ring; the characters of U with values in the Λ-module M and local conditions (Definition 7.3) [`XDual N U R M`]

$D_\infty(\ell,N,U)$, $X_\infty(\ell,N,U)$ the case of $U_{\ell,\infty}$ and $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ [`Dinf l N U`]; its dual [`Xinf l N U`], the Iwasawa module for $N=\ell$ and the whole group

$D_\infty(\ell,N,U)(-h)$, $X_\infty(\ell,N,U)(h)$ the two modules with the twisted actions [`dTw l N U e`, `xTw l N U e`]

$D_\infty(\ell,N,U)(-h)^V$ the elements of the first of them fixed by V [`ShaD l N U V e`]

$\mathcal{Q}_\ell^{\overline{F}/F}(-h)$, $\mathcal{Q}(\mathscr{D})(-h)$, $\mathbb{Z}_\ell(h)$ Tate twists: $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ with the action of $\mathrm{Gal}(\overline{F}/F)$ through the $(-h)$-th power of the cyclotomic character [`qzG F Ω l e`]; the same for the group of a local datum [`qzTw D e`]; $\mathbb{Z}_\ell$ with the h-th power

$Ш^1_\ell(F,h)$, $\operatorname{len} Ш^1_\ell(F,h)$ classes trivial above ℓ and unramified elsewhere (Definition 7.6); the length of this group [`shaInv F l e`]

$\mathscr{D}$, $\Gamma_\mathscr{D}$, $H^i(\mathscr{D},\cdot)$ a local datum of F at ℓ [`D : LData F Ω l`]; the Galois group unramified outside ℓ and infinity, formed in the closure of the datum; its continuous cohomology

$Ш^1(\mathscr{D},h)$, $\operatorname{len} H^2\big(\mathscr{D},\mathbb{Z}_\ell(h+1)\big)$ the classes in the description by a local datum [`Sha D e`]; the length of $H^2(\mathscr{D},\mathbb{Z}_\ell(h+1))$ [`VLen D e`]

μ, R_ℓ Iwasawa's invariant (§7); number of generators for ℓ

q, Δ, p, p' a modulus, a subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$; two primes (Proposition 7.18)

C, d_L, $[L:\mathbb{Q}]$, $\#$ a constant; discriminant and degree of L; number of elements (Definition 7.19)

θ, Θ, Ξ, J, Y, ω the real numbers of Lemma 7.20

$\Phi(T)$, s characteristic polynomial; an ℓ-adic variable (Remark 7.22)

E in §1, the number field of the guide

References

[Al] L. Alpöge, announcement of proofs of the Riemann hypothesis and of the generalized Riemann hypothesis for Dirichlet characters, 20 November 2026, with a Lean archive; public mirror of the archive at commit `40e56bab`.

[At] Riemann proof atlas: the declarations of the archive on a map of arXiv papers; data at commit `d05bd171`.

[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.

[Gu] *The proof of the Riemann hypothesis announced by L. Alpöge: a guide to its architecture*, riemann-rev, `guide/proof-guide.pdf`.

[Iw] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, *Ann. of Math.* (2) **98** (1973), 246–326.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.

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

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