DEFORMALIZATION 3

Descent to a layer of the cyclotomic tower

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

Summary. Let F be a number field with algebraic closure Ω, and let ℓ be a prime. The group $\mathrm{Gal}(\Omega/F)$ acts by conjugation on the module of the locally constant characters of the kernel of its ℓ-adic cyclotomic character with values in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, and this action can be twisted by a power of the cyclotomic character. We prove two statements that the first note of this series [N1] used as inputs. First, for a finite extension E of F inside the cyclotomic tower, restriction identifies the locally trivial classes of Galois cohomology over E with the characters fixed by the twisted action of the subgroup that belongs to E; here two theorems on restriction are taken from a neighbouring unit of the archive. Second, these fixed elements are the kernel of one operator $T - 1$, where T is the twisted action of an element whose cyclotomic value generates the image of the group. On the way we describe which roots of unity of ℓ-power order a number field contains in terms of the cyclotomic character.

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. The reading project divides the part of the archive that the final theorems use into units. This note treats one unit, on the layers of the cyclotomic tower and the twisted actions: all 39 of its declarations that the final theorems use. Three results are taken from other units and stated as Inputs G, R1 and R2; they are not proved here. Everything else is proved in full. Every statement was compared with its formal counterpart at commit `40e56bab` of the public mirror; Appendix A is the concordance of 70 declarations. The proofs were written from the structured proofs of the reading project (§11).

1 The statements

The first note [N1] bounded the lengths of groups of locally trivial Galois cohomology along the cyclotomic tower of a number field. It reduced them to cokernels of one operator on an Iwasawa module, and for this it needed two facts about the dual module, its Inputs 2a and 2b. Both are theorems of the unit of the archive treated here. The notation is set up in §2, and every function that the archive defines is written with all the arguments of its formal definition. In particular, for a prime ℓ, a number field F with algebraic closure Ω, a subgroup H of $\mathrm{Gal}(\Omega/F)$ and integers $N \geq 0$ and h, the group $H_{\ell,\infty}$ is the intersection of H with the kernel of the cyclotomic character $\kappa_\ell^{\Omega/F}(\cdot)$; the module $D_\infty(\ell, N, H)$ consists of characters of $H_{\ell,\infty}$; the twisted action of $g \in \mathrm{Gal}(\Omega/F)$ on it, when H is normal, is

$$T_{\ell,N,H;h}(g)\,\varphi = \kappa_\ell^{\Omega/F}(g)^{-h}\,\rho_{\ell,N,H}(g)\,\varphi,$$

where $\rho_{\ell,N,H}(g)$ is conjugation by g; and $D_\infty(\ell, N, H)(-h)^V$ is the module of the elements fixed by $T_{\ell,N,H;h}(g)$ for all g in a subgroup V.

Theorem A (descent). *In Setting 2.4, let $\mathscr{D} \in \mathrm{Dat}_\ell(\Omega/E)$ be a datum for the field E (Definition 8.1), let $h \neq 0$ be an integer, and assume that condition $\mathrm{P}_\ell(\Omega/E)$ holds: ℓ is odd, or $\kappa_\ell^{\Omega/E}(\mathrm{Gal}(\Omega/E)) \subseteq U_\ell^{(2)}$. Let H be a normal subgroup of $\mathrm{Gal}(\Omega/F)$ with $H_{\ell,\infty} = \mathrm{Gal}_F(\Omega/E)_{\ell,\infty}$. Then there is an isomorphism of $\mathbb{Z}_\ell$-modules*

$$\Phi : \; Ш^1(\mathscr{D}, h) \longrightarrow D_\infty(\ell, \ell, H)(-h)^{\mathrm{Gal}_F(\Omega/E)}$$

that is given by restriction for E, $\mathscr{D}$, h and H (Definition 8.3): $(\Phi\xi)(u') = \mathrm{res}_\infty(\mathscr{D}, h; \xi)(u)$ for all $\xi \in Ш^1(\mathscr{D}, h)$, all $u \in \mathrm{Gal}(\Omega/E)_{\ell,\infty}$ and all $u' \in H_{\ell,\infty}$ with $u' = \iota_{E/F}^{\Omega}(u)$.

Theorem B (invariants). *In Setting 2.1, let H be a closed normal subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ and h be integers, and let V be a subgroup of H. Let γ be an ℓ-generator for V (Definition 2.10): $\gamma \in V$, and $\kappa_\ell^{\Omega/F}(V)$ lies in the closure of the set of powers $\kappa_\ell^{\Omega/F}(\gamma)^j$, $j \in \mathbb{Z}$. Then*

$$D_\infty(\ell, N, H)(-h)^V = \ker\big(T_{\ell,N,H;h}(\gamma) - 1\big) = \ker\big(T_{\ell,N,H;h}(\gamma^{-1}) - 1\big).$$

LEAN A `Tower.desc`, in the form `Tower.IsDesc` · B `Tower.shaDGen`

In Theorem A the fields, the prime, the datum $\mathscr{D}$, the integer h and the group H are given first, and the isomorphism Φ is asserted for them. By Proposition 5.2(a) the map $\iota_{E/F}^{\Omega}(\cdot)$, which regards an automorphism of Ω over E as one over F, carries $\mathrm{Gal}(\Omega/E)_{\ell,\infty}$ bijectively onto $\mathrm{Gal}_F(\Omega/E)_{\ell,\infty} = H_{\ell,\infty}$. So $\Phi\xi$ is the map $\mathrm{res}_\infty(\mathscr{D}, h; \xi)$ read on $H_{\ell,\infty}$: the theorem says that restriction takes the locally trivial classes into the invariants, and that it is an isomorphism onto them.

The data $\mathscr{D}$, the group $Ш^1(\mathscr{D}, h)$ of locally trivial classes and the restriction map are recalled in §8. In Theorem A the case $H = \mathrm{Gal}(\Omega/F)$ is the one used in [N1]: there the hypothesis on H says that $\mathrm{Gal}(\Omega/F)_{\ell,\infty} \subseteq \mathrm{Gal}_F(\Omega/E)$, that is, that E lies in the field generated over F by all roots of unity of ℓ-power order in Ω. Theorem A rests on two theorems on the restriction map, Inputs R1 and R2 of §8; they carry its arithmetic content and belong to another unit. Theorem B is proved in full, from the local constancy established in the second note [N2].

2 The setting

Conventions. Rings are commutative, and a module is a module over the ring that is named. A *representation* of a group Γ on a module M over a ring Λ is a homomorphism from Γ to the monoid of the Λ-linear maps $M \to M$. For a prime number ℓ we write $\mathbb{Z}_\ell$ for the ring of ℓ-adic integers, $\mathbb{Q}_\ell$ for its field of fractions and $\mathbb{Z}_\ell^\times$ for the group of units of $\mathbb{Z}_\ell$ with its ℓ-adic topology. A *number field* is a field of finite degree over $\mathbb{Q}$. When a field Ω is called an algebraic closure of a field F, an embedding of F into Ω belongs to it, and F is regarded as a subfield of Ω. A *finite extension of F in Ω* is a subfield E of Ω that contains F and has finite degree over it; the embeddings of F into E and of E into Ω are compatible with the one of F into Ω. A subgroup of a topological group carries the induced topology. The *length* $\mathrm{len}\, M$ of a module M is the supremum of the lengths of its chains of submodules, a non-negative integer or ∞.

A statement of this note either states all its hypotheses itself, or it cites one of three Settings that hold them: the next one, Setting 2.4, and Setting 7.1 of §7.

Setting 2.1. ℓ is a prime number, F is a number field, and Ω is an algebraic closure of F.

Definition 2.2 (the group, the coefficients, the character). In Setting 2.1, $\mathrm{Gal}(\Omega/F)$ is the group of the automorphisms of the field Ω that fix every element of F, with its usual topology, in which the subgroups of the elements that fix a finite extension of F in Ω are a basis of neighbourhoods of 1. This group is compact [NSW, Ch. I, §1]. The group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the quotient of $\mathbb{Q}_\ell$ by $\mathbb{Z}_\ell$, a module over $\mathbb{Z}_\ell$. The *ℓ-adic cyclotomic character* of Ω over F is the continuous homomorphism

$$\kappa_\ell^{\Omega/F}(\cdot):\quad \mathrm{Gal}(\Omega/F)\longrightarrow \mathbb{Z}_\ell^\times \qquad \text{with} \qquad g(\zeta)=\zeta^{\kappa_\ell^{\Omega/F}(g)}$$

for every $g\in\mathrm{Gal}(\Omega/F)$ and every root of unity ζ of ℓ-power order in Ω. For a subgroup H of $\mathrm{Gal}(\Omega/F)$ we write $\kappa_\ell^{\Omega/F}(H)$ for its image, the group of the values $\kappa_\ell^{\Omega/F}(g)$ with $g\in H$.

LEAN G · QZ · Gal.cycZ

Definition 2.3 (levels). In Setting 2.1, let $n\ge 0$ be an integer and H a subgroup of $\mathrm{Gal}(\Omega/F)$.

(i) $U_\ell^{(n)}$ is the group of the units of $\mathbb{Z}_\ell$ that are congruent to 1 modulo ℓ^n. So $U_\ell^{(n)}=1+\ell^n\mathbb{Z}_\ell$ for $n\ge 1$, and $U_\ell^{(0)}=\mathbb{Z}_\ell^\times$.

(ii) The subgroups of H of level n and of infinite level are

$$H_{\ell,n}=\{g\in H\ :\ \kappa_\ell^{\Omega/F}(g)\in U_\ell^{(n)}\},\qquad H_{\ell,\infty}=\{g\in H\ :\ \kappa_\ell^{\Omega/F}(g)=1\}.$$

For the whole group, $\mathrm{Gal}(\Omega/F)_{\ell,n}$ consists of all $g\in\mathrm{Gal}(\Omega/F)$ with $\kappa_\ell^{\Omega/F}(g)\in U_\ell^{(n)}$, and $\mathrm{Gal}(\Omega/F)_{\ell,\infty}$ is the kernel of $\kappa_\ell^{\Omega/F}(\cdot)$.

(iii) $q_\ell=2$ if $\ell=2$, and $q_\ell=1$ if ℓ is odd, so that ℓ^{q_ℓ} is 4 or ℓ. The group H_{ℓ,q_ℓ} is the subgroup of H of level q_ℓ.

(iv) *Condition* $\mathrm{P}_\ell(\Omega/F)$ *holds* if ℓ is odd or $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F))\subseteq U_\ell^{(2)}$. For $\ell=2$ this says that $\mathrm{Gal}(\Omega/F)_{\ell,q_\ell}$ is the whole group.

LEAN princ · Base.levU · Base.cycU · Kum.Un · Base.qExp · Base.gamU · Kum.Procyc

Setting 2.4. ℓ is a prime number, F is a number field, Ω is an algebraic closure of F, and E is a finite extension of F in Ω. Then E is a number field and Ω is an algebraic closure of E, so that Setting 2.1 holds for E in the place of F as well.

Definition 2.5 (the subgroup of an extension). In Setting 2.4, $\mathrm{Gal}_F(\Omega/E)$ is the subgroup of the $g\in\mathrm{Gal}(\Omega/F)$ that fix every element of E. An element g of $\mathrm{Gal}(\Omega/E)$ fixes every element of F; regarded as an element of $\mathrm{Gal}(\Omega/F)$ it is written $\iota_{E/F}^{\Omega}(g)$. The map $\iota_{E/F}^{\Omega}(\cdot):\ \mathrm{Gal}(\Omega/E)\to\mathrm{Gal}(\Omega/F)$ is an injective homomorphism, and its image is $\mathrm{Gal}_F(\Omega/E)$.

LEAN Base.galOf · Base.galEmb

Definition 2.6 (characters). In Setting 2.1, a *valuation ring* of Ω is a subring A such that every $t\ne 0$ in Ω has t or t^{-1} in A. Its non-units form its maximal ideal $\mathfrak{m}_A$. The *decomposition group* of A is $G_A=\{g\in\mathrm{Gal}(\Omega/F)\ :\ g(A)=A\}$, and the *inertia group* I_A consists of the $g\in G_A$ with $g(t)-t\in\mathfrak{m}_A$ for all $t\in A$. Both are subgroups of $\mathrm{Gal}(\Omega/F)$ for the fields of the Setting: the notation shows the valuation ring only, and where two fields are in play the text says in which group they are formed.

Let C be a subgroup of $\mathrm{Gal}(\Omega/F)$, let $N\ge 0$ be an integer, Λ a ring and M a Λ-module. As in the definition of the modules of characters in the second note [N2, §2], $D_N(C;\Lambda,M)$ denotes the Λ-module of the maps $\varphi: C\to M$ that are locally constant, are additive,

$\varphi(uw) = \varphi(u) + \varphi(w)$, vanish on $C \cap I_A$ for every valuation ring A of Ω, and vanish on $C \cap G_A$ for every valuation ring A with $N \in \mathfrak{m}_A$. For a subgroup H of $\mathrm{Gal}(\Omega/F)$ we put

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

The prime, the integer N and the group H are written every time. When H is the whole group, the second module is $X_\infty(\ell, N, \mathrm{Gal}(\Omega/F))$. Let $\overline{F}$ be the algebraic closure of F that the library of the archive constructs; then $X_\infty(\ell, 1, \mathrm{Gal}(\overline{F}/F))$ and $X_\infty(\ell, \ell, \mathrm{Gal}(\overline{F}/F))$ are the modules with $N = 1$ and with $N = \ell$ for the whole group over $\overline{F}$. The modules of [N1] are those of the whole group with $N = \ell$.

LEAN `Kum.Dinf` · `Kum.Xinf` · for the whole group: `Tower.XN`, and its cases $N = 1$ and $N = \ell$ over the algebraic closure that the library provides, `Tower.XX` and `Tower.XP`

Definition 2.7 (actions). In Setting 2.1, let C be a normal subgroup of $\mathrm{Gal}(\Omega/F)$, Λ a ring and M a Λ-module. The group $\mathrm{Gal}(\Omega/F)$ acts by conjugation on the Λ-module of all maps $\varphi : C \to M$: the representation $\mathscr{F}_\Lambda(C, M)$ is given by

$$\big(\mathscr{F}_\Lambda(C, M)(g)\,\varphi\big)(u) = \varphi(g^{-1}ug) \qquad \text{for } g \in \mathrm{Gal}(\Omega/F),\ u \in C.$$

Let H be a normal subgroup of $\mathrm{Gal}(\Omega/F)$ and $N \geq 0$ an integer. Then $H_{\ell,\infty}$ is normal in $\mathrm{Gal}(\Omega/F)$, and by the proposition on conjugation of the second note [N2, §2] the operators $\mathscr{F}_{\mathbb{Z}_\ell}(H_{\ell,\infty}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)(g)$ map $D_\infty(\ell, N, H)$ into itself. Their restrictions to this module form the representation $\rho_{\ell,N,H}$ of $\mathrm{Gal}(\Omega/F)$ on $D_\infty(\ell, N, H)$; it is $\mathbb{Z}_\ell$-linear, and

$$\big(\rho_{\ell,N,H}(g)\,\varphi\big)(u) = \varphi(g^{-1}ug) \qquad \text{for } \varphi \in D_\infty(\ell, N, H),\ u \in H_{\ell,\infty}.$$

On $X_\infty(\ell, N, H)$ the group acts by the representation $\rho^\vee_{\ell,N,H}$ with

$$\big(\rho^\vee_{\ell,N,H}(g)\,x\big)(\varphi) = x\big(\rho_{\ell,N,H}(g^{-1})\,\varphi\big) \qquad \text{for } x \in X_\infty(\ell, N, H),\ \varphi \in D_\infty(\ell, N, H).$$

LEAN `Kum.funRep` · `Tower.dRep`, a restriction of `Kum.funRep` by `Kum.funRepMem` · `Tower.xRep`, `Tower.xRep_apply`

Definition 2.8 (twists and invariants). Let Λ be a ring, Γ a group, M a Λ-module, π a representation of Γ on M, and ω a homomorphism from Γ to the group of units of Λ. Scalars commute with Λ-linear maps, so $g \mapsto \omega(g)\,\pi(g)$ is again a representation of Γ on M. It is the *twist* $\pi \otimes \omega$ of π by ω.

In Setting 2.1, let H be a normal subgroup of $\mathrm{Gal}(\Omega/F)$, and let $N \geq 0$ and h be integers. The cyclotomic character $\kappa_\ell^{\Omega/F}(\cdot)$ is a homomorphism to the units of $\mathbb{Z}_\ell$, and so are its powers. We put

$$T_{\ell,N,H;h} = \rho_{\ell,N,H} \otimes \kappa_\ell^{\Omega/F}(\cdot)^{-h}, \qquad T^\vee_{\ell,N,H;h} = \rho^\vee_{\ell,N,H} \otimes \kappa_\ell^{\Omega/F}(\cdot)^{h},$$

so that for $g \in \mathrm{Gal}(\Omega/F)$

$$T_{\ell,N,H;h}(g) = \kappa_\ell^{\Omega/F}(g)^{-h}\,\rho_{\ell,N,H}(g), \qquad T^\vee_{\ell,N,H;h}(g) = \kappa_\ell^{\Omega/F}(g)^{h}\,\rho^\vee_{\ell,N,H}(g).$$

We write $D_\infty(\ell, N, H)(-h)$ for the module $D_\infty(\ell, N, H)$ with the action $T_{\ell,N,H;h}$ of $\mathrm{Gal}(\Omega/F)$, and $X_\infty(\ell, N, H)(h)$ for the module $X_\infty(\ell, N, H)$ with the action $T^\vee_{\ell,N,H;h}$. For a subgroup V of $\mathrm{Gal}(\Omega/F)$ the module of invariants is

$$D_\infty(\ell, N, H)(-h)^V = \big\{\varphi \in D_\infty(\ell, N, H) \,:\, T_{\ell,N,H;h}(g)\,\varphi = \varphi \text{ for all } g \in V\big\}.$$

LEAN `Tower.twist` · `Tower.dTw`, `Tower.dTw_apply` · `Tower.xTw`, `Tower.xTw_apply` · `Tower.ShaD`

Lemma 2.9. *In Setting 2.1, let H be a normal subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ and h be integers, and let $g \in \mathrm{Gal}(\Omega/F)$, $x \in X_\infty(\ell, N, H)$ and $\varphi \in D_\infty(\ell, N, H)$. Then*

$$\big(T^\vee_{\ell,N,H;h}(g)\,x\big)(\varphi) = x\big(T_{\ell,N,H;h}(g^{-1})\,\varphi\big).$$

Proof. The left side is $\kappa_\ell^{\Omega/F}(g)^h\, x\big(\rho_{\ell,N,H}(g^{-1})\,\varphi\big)$ by Definitions 2.7 and 2.8. Since $\kappa_\ell^{\Omega/F}(g)^h = \kappa_\ell^{\Omega/F}(g^{-1})^{-h}$ and x is $\mathbb{Z}_\ell$-linear, this is the right side. □

LEAN `Tower.xTw_apply_apply`

Definition 2.10. In Setting 2.1, let V be a subgroup of $\mathrm{Gal}(\Omega/F)$. An element $\gamma \in V$ is an *ℓ-generator for V* if $\kappa_\ell^{\Omega/F}(V)$ is contained in the closure of the set $\{\kappa_\ell^{\Omega/F}(\gamma)^j : j \in \mathbb{Z}\}$ in $\mathbb{Z}_\ell^\times$.

LEAN `Tower.IsGen`

Definition 2.11 (layers). In Setting 2.1, $a_\ell(F)$ is the largest integer $c \geq 0$ such that F contains a primitive root of unity of order ℓ^c; it exists by Lemma 3.2. For an integer $n \geq 0$ let $\mu_{\ell^n}(\Omega)$ be the set of the $t \in \Omega$ with $t^{\ell^n} = 1$. For $m \geq 0$ the *layer* of index m of F in Ω is the field

$$F\big(\mu_{\ell^{a_\ell(F)+m}}(\Omega)\big)$$

generated over F by the set $\mu_{\ell^n}(\Omega)$ for $n = a_\ell(F) + m$, that is, by the roots of unity in Ω whose order divides this power of ℓ. Its group is $\mathrm{Gal}(\Omega/F)_{\ell,\,a_\ell(F)+m}$ (Lemma 3.1).

LEAN `Tower.cZero` · `Tower.layU` · `Tower.layF`

Definition 2.12 (the tower condition). The main theorem of [N1] is stated with the following notions.

(i) Let Λ be a ring, M a Λ-module and $n \geq 0$ an integer. The module M is *generated by at most n elements over Λ* if it is the image of a Λ-linear map from the free module of rank n; it is then finitely generated.

(ii) The archive measures a Λ-linear map $\alpha : M \to M$ by the length of its cokernel $M/\alpha(M)$ as a Λ-module, a non-negative integer or ∞.

(iii) In Setting 2.1, let H be a subgroup of $\mathrm{Gal}(\Omega/F)$ and $N \geq 0$ an integer. The elements of $D_\infty(\ell, N, H)$ that are killed by ℓ form the submodule $D_\infty(\ell, N, H)[\ell]$, and its length as a $\mathbb{Z}_\ell$-module is written $\mathrm{len}\, D_\infty(\ell, N, H)[\ell]$.

(iv) Let ℓ be a prime number, F a number field and R an integer. The *tower condition holds for ℓ, F and R* if the field F is totally complex, it contains a primitive root of unity of order ℓ^{q_ℓ}, $R \geq 1$, and the module $X_\infty(\ell, \ell, \mathrm{Gal}(\overline{F}/F))$ is generated by at most R elements over $\mathbb{Z}_\ell$. This is the standing hypothesis of that theorem.

LEAN `Tower.GenLE`, `Tower.GenLE.finite` · `Tower.cokerLen` · `Tower.xRank` · `Tower.IsTower`, with `HasMuQ` for the root of unity of order ℓ^{q_ℓ}

3 Roots of unity and levels

Lemma 3.1. *In Setting 2.1, let $g \in \mathrm{Gal}(\Omega/F)$ and let $n \geq 0$ be an integer. Then $\kappa_\ell^{\Omega/F}(g) \in U_\ell^{(n)}$ if and only if $g(t) = t$ for every $t \in \Omega$ with $t^{\ell^n} = 1$.*

Proof. For $n = 0$ both conditions hold. Let $n \geq 1$. The field Ω is algebraically closed of characteristic zero, so the $t \in \Omega$ with $t^{\ell^n} = 1$ form a cyclic group of order ℓ^n; let ζ be a generator. By the definition of the cyclotomic character we have $g(t) = t^{\kappa_\ell^{\Omega/F}(g)}$ for these t, where

the exponent matters only modulo ℓ^n. If $\kappa_\ell^{\Omega/F}(g) \equiv 1$ modulo ℓ^n, then $g(t) = t$. Conversely, $g(\zeta) = \zeta$ gives $\zeta^{\kappa_\ell^{\Omega/F}(g)-1} = 1$, so ℓ^n divides $\kappa_\ell^{\Omega/F}(g) - 1$. □

LEAN `cyc_mem_princ_iff`

Lemma 3.2. *Let ℓ be a prime number, F a number field and $c \geq 0$ an integer. If F contains a primitive root of unity of order ℓ^c, then $c \leq [F : \mathbb{Q}]$.*

Proof. Let $c \geq 1$. The minimal polynomial over $\mathbb{Q}$ of such a root is the cyclotomic polynomial of order ℓ^c, of degree $\ell^{c-1}(\ell - 1)$ [Wa, Thm. 2.5]. This degree is at most $[F : \mathbb{Q}]$, and $c \leq \ell^{c-1} \leq \ell^{c-1}(\ell - 1)$. □

LEAN `le_finrank`

Proposition 3.3. *In Setting 2.1 the following hold.*

(a) *For every integer $c \geq 0$ the following are equivalent: F contains a primitive root of unity of order ℓ^c; $c \leq a_\ell(F)$; $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F)) \subseteq U_\ell^{(c)}$, that is, $\mathrm{Gal}(\Omega/F)_{\ell,c}$ is the whole group $\mathrm{Gal}(\Omega/F)$.*

(b) *F contains a primitive root of unity of order ℓ^{q_ℓ} if and only if $q_\ell \leq a_\ell(F)$. In that case F is totally complex and condition $\mathrm{P}_\ell(\Omega/F)$ holds.*

(c) *Condition $\mathrm{P}_\ell(\Omega/F)$ holds if and only if ℓ is odd or F contains a primitive root of unity of order ℓ^{q_ℓ}, which for $\ell = 2$ is a primitive fourth root of unity.*

Proof. (a) Write $a = a_\ell(F)$. The integers c for which F contains a primitive root of unity of order ℓ^c include 0 and are bounded by Lemma 3.2, so there is a largest one, which is a. If ζ is such a root of order ℓ^a and $c \leq a$, then $\zeta^{\ell^{a-c}}$ has order ℓ^c. This gives the first equivalence. For the second, suppose $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F)) \subseteq U_\ell^{(c)}$, and let ζ be a primitive root of unity of order ℓ^c in Ω. By Lemma 3.1 it is fixed by $\mathrm{Gal}(\Omega/F)$, and the field of the elements fixed by $\mathrm{Gal}(\Omega/F)$ is F, so $\zeta \in F$. Conversely, if F contains a primitive root ζ of order ℓ^c, every $t \in \Omega$ with $t^{\ell^c} = 1$ is a power of ζ, hence fixed by $\mathrm{Gal}(\Omega/F)$, and Lemma 3.1 gives $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F)) \subseteq U_\ell^{(c)}$.

(b) The first assertion is (a) for $c = q_\ell$. A root of unity of order $\ell^{q_\ell} > 2$ is not real, so F has no embedding into the real numbers. If $\ell = 2$, then $q_\ell = 2$ and (a) gives $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F)) \subseteq U_\ell^{(2)}$.

(c) For odd ℓ both statements hold. For $\ell = 2$ condition $\mathrm{P}_\ell(\Omega/F)$ says $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F)) \subseteq U_\ell^{(2)}$, which by (a) means that F contains a primitive fourth root of unity. □

LEAN `Tower.muQ` · (a) `ex_iff`, `all_iff` · (b) the root of order ℓ^{q_ℓ}: `HasMuQ`

4 Torsion, and elements that act trivially

Proposition 4.1. *In Setting 2.1, let H be a subgroup of $\mathrm{Gal}(\Omega/F)$ and $N \geq 0$ an integer.*

(a) *If H is closed in $\mathrm{Gal}(\Omega/F)$, every element of $D_\infty(\ell, N, H)$ is killed by a power of ℓ.*

(b) *$D_\infty(\ell, N, H) \subseteq D_\infty(\ell, 1, H)$, and $\operatorname{len} D_\infty(\ell, N, H)[\ell] \leq \operatorname{len} D_\infty(\ell, 1, H)[\ell]$: the submodule of the elements killed by ℓ has at most the length of the corresponding submodule of $D_\infty(\ell, 1, H)$.*

(c) *If H is normal in $\mathrm{Gal}(\Omega/F)$ and $g \in H_{\ell,\infty}$, then $\rho_{\ell,N,H}(g)$ is the identity of $D_\infty(\ell, N, H)$ and $\rho^\vee_{\ell,N,H}(g)$ is the identity of $X_\infty(\ell, N, H)$, and so are $T_{\ell,N,H;h}(g)$ and $T^\vee_{\ell,N,H;h}(g)$ for every integer h.*

Proof. (a) An element of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the class of some $s \in \mathbb{Q}_\ell$, and $\ell^r s \in \mathbb{Z}_\ell$ for large r; so every element of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is killed by a power of ℓ. The group $H_{\ell,\infty}$ is the intersection of the closed

subgroup H with the kernel of the continuous map $\kappa_\ell^{\Omega/F}(\cdot)$, hence closed in the compact group $\mathrm{Gal}(\Omega/F)$, hence compact. A locally constant map on a compact space takes finitely many values. So one power of ℓ kills all values of a given φ.

(b) The conditions for $D_\infty(\ell, 1, H)$ are those for $D_\infty(\ell, N, H)$ without the last one, because 1 lies in no maximal ideal. An inclusion of modules restricts to the elements killed by ℓ, and the length of a submodule is at most that of the module.

(c) Let $\varphi \in D_\infty(\ell, N, H)$ and $u \in H_{\ell,\infty}$. The elements g^{-1}, u and g lie in $H_{\ell,\infty}$, and φ is additive, so

$$\big(\rho_{\ell,N,H}(g)\,\varphi\big)(u) = \varphi(g^{-1}ug) = \varphi(g^{-1}) + \varphi(u) + \varphi(g) = \varphi(u),$$

because $\varphi(g^{-1}) + \varphi(g) = \varphi(1) = 0$. Hence $\rho_{\ell,N,H}(g)$ fixes every φ. Then

$$\big(\rho^\vee_{\ell,N,H}(g)\,x\big)(\varphi) = x\big(\rho_{\ell,N,H}(g^{-1})\,\varphi\big) = x(\varphi) \qquad \text{for } x \in X_\infty(\ell, N, H),$$

as g^{-1} lies in $H_{\ell,\infty}$ too. Finally $\kappa_\ell^{\Omega/F}(g) = 1$, so the twists change nothing. □

LEAN `Tower.dinfTors`; the length in (b) is `Tower.xRank`

In (a), Theorem A of the second note [N2] proves the same statement; the archive has it in both units.

5 Generators

Input G (closed subgroups of the units). *Let ℓ be a prime number and W a closed subgroup of $\mathbb{Z}_\ell^\times$, and assume $W \subseteq U_\ell^{(2)}$ if $\ell = 2$. Then there is $s \in W$ such that the set of powers s^j, $j \in \mathbb{Z}$, is dense in W.*

LEAN `Kum.existsGen`

This is proved in another unit of the archive and is not deformalized here. It expresses the classical structure of the units: for odd ℓ the group $\mathbb{Z}_\ell^\times$ is the product of a cyclic group of order $\ell - 1$ and of $U_\ell^{(1)} \cong \mathbb{Z}_\ell$, and $U_2^{(2)} \cong \mathbb{Z}_2$ for $\ell = 2$ [Se, Ch. II, §3]; a closed subgroup of such a group is topologically generated by one element.

Proposition 5.1. *In Setting 2.1, let H be a closed subgroup of $\mathrm{Gal}(\Omega/F)$. Assume that ℓ is odd or that $H \subseteq \mathrm{Gal}(\Omega/F)_{\ell,q_\ell}$, that is, $\kappa_\ell^{\Omega/F}(H) \subseteq U_\ell^{(q_\ell)}$. Then there is an ℓ-generator for H.*

Proof. The group H is closed in the compact group $\mathrm{Gal}(\Omega/F)$, so it is compact, and its image $\kappa_\ell^{\Omega/F}(H)$ under the continuous map $\kappa_\ell^{\Omega/F}(\cdot)$ is compact, hence closed in $\mathbb{Z}_\ell^\times$. If $\ell = 2$, it lies in $U_\ell^{(2)}$, because $q_\ell = 2$. By Input G there is $s \in \kappa_\ell^{\Omega/F}(H)$ whose powers are dense in $\kappa_\ell^{\Omega/F}(H)$. Any $\gamma \in H$ with $\kappa_\ell^{\Omega/F}(\gamma) = s$ is an ℓ-generator for H. □

LEAN `Tower.existsGen`

Proposition 5.2. *In Setting 2.4 the following hold.*

(a) $\mathrm{Gal}_F(\Omega/E)$ *is open and closed in* $\mathrm{Gal}(\Omega/F)$, *and* $\kappa_\ell^{\Omega/E}(g) = \kappa_\ell^{\Omega/F}(\iota^\Omega_{E/F}(g))$ *for every* $g \in \mathrm{Gal}(\Omega/E)$.

(b) *Condition* $\mathrm{P}_\ell(\Omega/E)$ *holds if and only if* ℓ *is odd or* $\mathrm{Gal}_F(\Omega/E) \subseteq \mathrm{Gal}(\Omega/F)_{\ell,q_\ell}$.

(c) *If condition* $\mathrm{P}_\ell(\Omega/E)$ *holds, there is an* ℓ*-generator for* $\mathrm{Gal}_F(\Omega/E)$.

Proof. (a) The group $\mathrm{Gal}_F(\Omega/E)$ is one of the basic neighbourhoods of 1, so it is open; its complement is a union of cosets of it, so it is closed. Both characters describe the action on the same roots of unity of Ω. (b) For $\ell = 2$ condition $\mathrm{P}_\ell(\Omega/E)$ says $\kappa_\ell^{\Omega/E}(\mathrm{Gal}(\Omega/E)) \subseteq U_\ell^{(2)}$, which by (a) and Definition 2.5 means $\mathrm{Gal}_F(\Omega/E) \subseteq \mathrm{Gal}(\Omega/F)_{\ell,2}$, and $q_\ell = 2$. (c) This is Proposition 5.1 for $H = \mathrm{Gal}_F(\Omega/E)$, by (a) and (b). □

LEAN `Tower.genGal` · the subgroup of E: `Base.galOf`, the image of `Base.galEmb` · (a) by `Base.galEmbTop` and `Base.galEmbFam`

6 Proof of Theorem B

Let H, N, h, V and γ be as in the theorem, and let $\varphi \in D_\infty(\ell, N, H)$ with $T_{\ell,N,H;h}(\gamma)\,\varphi = \varphi$. We show that $T_{\ell,N,H;h}(g)\,\varphi = \varphi$ for every $g \in V$.

A level that fixes φ. The group H is closed and normal, so by Theorem A(i) of the second note [N2] there is $n \geq 0$ with $\rho_{\ell,N,H}(w)\,\varphi = \varphi$ for all $w \in H_{\ell,n}$. By Proposition 4.1(a) there is $r \geq 0$ with $\ell^r \varphi = 0$. Put $m = \max(n, r)$, and let $w \in H_{\ell,m}$. Then $\rho_{\ell,N,H}(w)\,\varphi = \varphi$, because $H_{\ell,m} \subseteq H_{\ell,n}$. Moreover $\kappa_\ell^{\Omega/F}(w)^{-h}$ lies in $U_\ell^{(m)} \subseteq U_\ell^{(r)}$, so $\kappa_\ell^{\Omega/F}(w)^{-h} = 1 + \ell^r s$ with $s \in \mathbb{Z}_\ell$, and

$$T_{\ell,N,H;h}(w)\,\varphi = (1 + \ell^r s)\,\varphi = \varphi.$$

Powers of γ. The $g \in \mathrm{Gal}(\Omega/F)$ with $T_{\ell,N,H;h}(g)\,\varphi = \varphi$ form a subgroup of $\mathrm{Gal}(\Omega/F)$, because $T_{\ell,N,H;h}$ is a representation. It contains γ, hence every power γ^j.

Elements of V. Let $g \in V$. The set $\kappa_\ell^{\Omega/F}(g)\,U_\ell^{(m)}$ is an open neighbourhood of $\kappa_\ell^{\Omega/F}(g)$ in $\mathbb{Z}_\ell^\times$, and $\kappa_\ell^{\Omega/F}(g)$ lies in the closure of the powers of $\kappa_\ell^{\Omega/F}(\gamma)$. So there is an integer j with $\kappa_\ell^{\Omega/F}(\gamma)^j \in \kappa_\ell^{\Omega/F}(g)\,U_\ell^{(m)}$. Put $w = \gamma^{-j} g$. Then $w \in V \subseteq H$ and $\kappa_\ell^{\Omega/F}(w) \in U_\ell^{(m)}$, so $w \in H_{\ell,m}$. Since $g = \gamma^j w$,

$$T_{\ell,N,H;h}(g)\,\varphi = T_{\ell,N,H;h}(\gamma^j)\,T_{\ell,N,H;h}(w)\,\varphi = T_{\ell,N,H;h}(\gamma^j)\,\varphi = \varphi.$$

This shows $\ker\bigl(T_{\ell,N,H;h}(\gamma) - 1\bigr) \subseteq D_\infty(\ell, N, H)(-h)^V$. The other inclusion holds because $\gamma \in V$. Finally $T_{\ell,N,H;h}(\gamma^{-1})$ is the inverse of $T_{\ell,N,H;h}(\gamma)$, so the two operators fix the same elements. □

LEAN `Tower.shaDGen`, with `Kum.dinfNil` for the integer n

7 Transport of characters

The archive compares the modules of characters of two number fields with two algebraic closures.

Setting 7.1. F and F' are number fields, Ω is an algebraic closure of F and Ω' is an algebraic closure of F', $f\colon F \to F'$ is a homomorphism of fields, and $\tau\colon \Omega \to \Omega'$ is an isomorphism of fields that extends f: $\tau(t) = f(t)$ for all $t \in F$.

Lemma 7.2. *In Setting 7.1, for $g' \in \mathrm{Gal}(\Omega'/F')$ the map $\theta(g') = \tau^{-1} g' \tau$ is an automorphism of Ω that fixes every element of F. The map*

$$\theta\colon \mathrm{Gal}(\Omega'/F') \to \mathrm{Gal}(\Omega/F), \qquad \tau\bigl(\theta(g')\,t\bigr) = g'(\tau t) \quad \text{for } t \in \Omega,$$

is an injective continuous homomorphism, and it is the only map with this property. For every prime number ℓ and every $g' \in \mathrm{Gal}(\Omega'/F')$ we have $\kappa_\ell^{\Omega/F}(\theta(g')) = \kappa_\ell^{\Omega'/F'}(g')$.

Proof. The map $\tau^{-1}g'\tau$ fixes F, because g' fixes $f(F)$. The displayed equation determines $\theta(g')$, and θ is a homomorphism; it is injective because τ is bijective. It is continuous: the elements that θ maps into $\mathrm{Gal}_F(\Omega/E)$, for a finite extension E of F in Ω, are those that fix $\tau(E)$, and these form an open subgroup of $\mathrm{Gal}(\Omega'/F')$. Since τ maps roots of unity to roots of unity, $\kappa_\ell^{\Omega/F}(\theta(g'))$ and $\kappa_\ell^{\Omega'/F'}(g')$ are the same exponent. □

LEAN `galTransport`; the formal statement has one more clause, not used here: θ is surjective if f is

Lemma 7.3. *In Setting 7.1, let θ be the homomorphism of Lemma 7.2, let A' be a valuation ring of Ω', and let $A = \tau^{-1}(A')$, a valuation ring of Ω. The groups G_A and I_A are formed in $\mathrm{Gal}(\Omega/F)$, the groups $G_{A'}$ and $I_{A'}$ in $\mathrm{Gal}(\Omega'/F')$.*

(a) *An element $t \in \Omega$ lies in $\mathfrak{m}_A$ if and only if $\tau(t)$ lies in $\mathfrak{m}_{A'}$; that is, $\mathfrak{m}_A = \tau^{-1}(\mathfrak{m}_{A'})$. In particular an integer lies in $\mathfrak{m}_A$ if and only if it lies in $\mathfrak{m}_{A'}$.*

(b) *Let $g' \in \mathrm{Gal}(\Omega'/F')$ and $g = \theta(g')$, so that $\tau(g(t)) = g'(\tau(t))$ for $t \in \Omega$. Then $g \in G_A$ if and only if $g' \in G_{A'}$, and $g \in I_A$ if and only if $g' \in I_{A'}$.*

Proof. (a) An element t lies in $\mathfrak{m}_A$ if and only if $t \in A$ and either $t = 0$ or $t^{-1} \notin A$. The isomorphism τ respects zero and inverses and maps A onto A'. It fixes the integers. (b) Since $g = \tau^{-1}g'\tau$, we have $g(A) = \tau^{-1}\big(g'(A')\big)$, which equals $A = \tau^{-1}(A')$ if and only if $g'(A') = A'$. For $t \in A$ we have $\tau(g(t) - t) = g'(\tau t) - \tau t$, and τt runs through A'. By (a) the left side lies in $\mathfrak{m}_{A'}$ exactly when $g(t) - t \in \mathfrak{m}_A$. □

LEAN (a) `dt_val_lt_one` · (b) `dt_dec`, `dt_ine`

Proposition 7.4. *In Setting 7.1, let $\theta\colon\ \mathrm{Gal}(\Omega'/F') \to \mathrm{Gal}(\Omega/F)$ be the homomorphism of Lemma 7.2, the one with $\tau(\theta(g')\,t) = g'(\tau(t))$ for all g' and all $t \in \Omega$. Let ℓ be a prime number and $N \geq 0$ an integer, and let H be a subgroup of $\mathrm{Gal}(\Omega/F)$ and H' a subgroup of $\mathrm{Gal}(\Omega'/F')$ with $\theta(H'_{\ell,\infty}) = H_{\ell,\infty}$. Then the map $\varphi \mapsto \varphi \circ \theta$ is an isomorphism of $\mathbb{Z}_\ell$-modules from $D_\infty(\ell, N, H)$ onto $D_\infty(\ell, N, H')$.*

Proof. A continuous injective map from a compact space to a Hausdorff space is a homeomorphism onto its image. So θ restricts to an isomorphism of topological groups from $H'_{\ell,\infty}$ onto $H_{\ell,\infty}$. Let $\varphi \in D_\infty(\ell, N, H)$. Then $\varphi \circ \theta$ is locally constant and additive. Let A' be a valuation ring of Ω' and $A = \tau^{-1}(A')$, with the four groups formed as in Lemma 7.3. If $g' \in H'_{\ell,\infty}$ lies in $I_{A'}$, then $\theta(g')$ lies in $H_{\ell,\infty} \cap I_A$ by Lemma 7.3(b), so $\varphi(\theta(g')) = 0$. If $N \in \mathfrak{m}_{A'}$ and g' lies in $G_{A'}$, then $N \in \mathfrak{m}_A$ and $\theta(g') \in H_{\ell,\infty} \cap G_A$, so again $\varphi(\theta(g')) = 0$. Hence $\varphi \circ \theta$ lies in $D_\infty(\ell, N, H')$. In the same way composition with the inverse of the restricted map carries the second module into the first: every valuation ring of Ω is $\tau^{-1}(A')$ for the valuation ring $A' = \tau(A)$, and Lemma 7.3 is an equivalence. The two maps are linear and inverse to each other. □

LEAN `Tower.dinfTransport`, with `dt_mem` for the four conditions

We use the proposition in one case. In Setting 2.4, take E for the second field, Ω for both algebraic closures, the inclusion of F in E for the homomorphism of fields and the identity of Ω for the isomorphism. Then the map of Lemma 7.2 is $\iota^{\Omega}_{E/F}(\cdot)\colon\ \mathrm{Gal}(\Omega/E) \to \mathrm{Gal}(\Omega/F)$, and the proposition says that for subgroups H of $\mathrm{Gal}(\Omega/F)$ and H' of $\mathrm{Gal}(\Omega/E)$ such that this map carries $H'_{\ell,\infty}$ onto $H_{\ell,\infty}$, composition with it identifies $D_\infty(\ell, N, H)$ with $D_\infty(\ell, N, H')$: it does not matter whether the decomposition and inertia groups are taken in $\mathrm{Gal}(\Omega/E)$ or in $\mathrm{Gal}(\Omega/F)$. This case can also be seen directly, since an element g of $\mathrm{Gal}(\Omega/E)$ lies in the group G_A or I_A formed in $\mathrm{Gal}(\Omega/E)$ exactly when $\iota^{\Omega}_{E/F}(g)$ lies in the group G_A or I_A formed in $\mathrm{Gal}(\Omega/F)$.

8 Proof of Theorem A

Definition 8.1 (the classes). In Setting 2.1, let S be the set of the prime ideals of the ring of integers of F that contain ℓ. Let $G_S(\Omega)$ be the quotient of $\mathrm{Gal}(\Omega/F)$ by the closed normal subgroup generated by the inertia groups I_A, for the valuation rings $A \neq \Omega$ of Ω with $\ell \notin \mathfrak{m}_A$; it is the Galois group of the largest extension of F in Ω that is unramified at the primes outside S. The cyclotomic character $\kappa_\ell^{\Omega/F}(\cdot)$ factors through $G_S(\Omega)$.

A *datum* for ℓ, F and Ω consists of the set S, of a valuation ring $A_\mathfrak{p}$ of Ω for each $\mathfrak{p} \in S$ whose maximal ideal contains $\mathfrak{p}$, and of the homomorphism $\chi\colon G_S(\Omega) \to \mathbb{Z}_\ell^\times$ whose composite with the projection $\mathrm{Gal}(\Omega/F) \to G_S(\Omega)$ is $\kappa_\ell^{\Omega/F}(\cdot)$; the archive carries this factorization as part of its data. The set of these data is $\mathrm{Dat}_\ell(\Omega/F)$. Let $\mathscr{D} \in \mathrm{Dat}_\ell(\Omega/F)$ be a datum, with valuation rings $A_\mathfrak{p}$ and homomorphism χ, and let h be an integer.

(i) $\mathscr{A}(\mathscr{D})(-h)$ is the module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ on which $g \in G_S(\Omega)$ acts as multiplication by $\chi(g)^{-h}$. The group $H^1(\mathscr{A}(\mathscr{D})(-h))$ consists of the continuous maps z from $G_S(\Omega)$ to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ with $z(gw) = z(g) + \chi(g)^{-h} z(w)$, modulo those of the form $g \mapsto \chi(g)^{-h} y - y$ with $y \in \mathbb{Q}_\ell/\mathbb{Z}_\ell$.

(ii) $Ш^1(\mathscr{D}, h)$ is the submodule of the classes in $H^1(\mathscr{A}(\mathscr{D})(-h))$ whose restriction to the image of the decomposition group $G_{A_\mathfrak{p}}$ in $G_S(\Omega)$ is trivial for each $\mathfrak{p} \in S$ [N1, §7]. These are the *locally trivial classes*.

(iii) On the kernel $\mathrm{Gal}(\Omega/F)_{\ell,\infty}$ of $\kappa_\ell^{\Omega/F}(\cdot)$ the action on $\mathscr{A}(\mathscr{D})(-h)$ is trivial. So the composite of a map z as in (i) with the projection $\mathrm{Gal}(\Omega/F) \to G_S(\Omega)$, restricted to $\mathrm{Gal}(\Omega/F)_{\ell,\infty}$, is a homomorphism $\mathrm{Gal}(\Omega/F)_{\ell,\infty} \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$, and it depends only on the class ξ of z. We call it $\mathrm{res}_\infty(\mathscr{D}, h; \xi)$.

(iv) $\mathscr{A}_\ell^{\Omega/F}(-h)$ is the module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ on which $g \in \mathrm{Gal}(\Omega/F)$ acts as multiplication by $\kappa_\ell^{\Omega/F}(g)^{-h}$.

LEAN `LData` · `qzTw` · `Sha` · `Kum.resInf` · the action in (iv): `qzG`

Definition 8.2 (equivariant characters). In Setting 2.1, let C be a subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ be an integer, Λ a ring, M a Λ-module and π a representation of $\mathrm{Gal}(\Omega/F)$ on M. Then $\mathscr{E}_N(C; \pi)$ is the Λ-module of all $\psi \in D_N(C; \Lambda, M)$ such that

$$\psi(gug^{-1}) = \pi(g)\,\psi(u) \qquad \text{for all } g \in \mathrm{Gal}(\Omega/F) \text{ and } u \in C \text{ with } gug^{-1} \in C.$$

LEAN `Kum.EqHom`

Input R1 (restriction is injective). *In Setting 2.1, let $\mathscr{D} \in \mathrm{Dat}_\ell(\Omega/F)$ be a datum (Definition 8.1) and $h \neq 0$ an integer, and assume that condition $\mathrm{P}_\ell(\Omega/F)$ holds. Then $\xi \mapsto \mathrm{res}_\infty(\mathscr{D}, h; \xi)$ is injective on $H^1(\mathscr{A}(\mathscr{D})(-h))$.*

Input R2 (the image of restriction). *In Setting 2.1, let $\mathscr{D} \in \mathrm{Dat}_\ell(\Omega/F)$ be a datum and $h \neq 0$ an integer, and assume that condition $\mathrm{P}_\ell(\Omega/F)$ holds. Then the image of $Ш^1(\mathscr{D}, h)$ under $\xi \mapsto \mathrm{res}_\infty(\mathscr{D}, h; \xi)$ is the module $\mathscr{E}_\ell(\mathrm{Gal}(\Omega/F)_{\ell,\infty}; \mathscr{A}_\ell^{\Omega/F}(-h))$ of Definition 8.2: the module of all $\psi \in D_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))$ such that*

$$\psi(gug^{-1}) = \kappa_\ell^{\Omega/F}(g)^{-h}\,\psi(u) \qquad \textit{for all } g \in \mathrm{Gal}(\Omega/F),\ u \in \mathrm{Gal}(\Omega/F)_{\ell,\infty}.$$

LEAN R1 `Kum.resInfInj` · R2 `Kum.resInfOnto`, with the module `Kum.EqHom`

Both are theorems of the unit of the archive on Kummer theory, the unit of [N2]; they are not deformalized here. The classical reason is the inflation and restriction sequence for the subgroup $\mathrm{Gal}(\Omega/F)_{\ell,\infty}$: the quotient of $\mathrm{Gal}(\Omega/F)$ by it is isomorphic to the group $\kappa_\ell^{\Omega/F}(\mathrm{Gal}(\Omega/F))$, which is topologically generated by one element under condition $\mathrm{P}_\ell(\Omega/F)$, and for $h \neq 0$ this element acts on $\mathcal{Q}_\ell^{\Omega/F}(-h)$ by a scalar different from 1 [NSW, Ch. I, §6].

Definition 8.3 (given by restriction). In Setting 2.4, let $\mathscr{D} \in \mathrm{Dat}_\ell(\Omega/E)$ be a datum for the field E, h an integer, H a normal subgroup of $\mathrm{Gal}(\Omega/F)$, and

$$\Phi : \ Ш^1(\mathscr{D}, h) \longrightarrow D_\infty(\ell, \ell, H)(-h)^{\mathrm{Gal}_F(\Omega/E)}$$

a homomorphism of $\mathbb{Z}_\ell$-modules. We say that Φ is *given by restriction for E, $\mathscr{D}$, h and H* if $(\Phi\xi)(u') = \mathrm{res}_\infty(\mathscr{D}, h; \xi)(u)$ for all $\xi \in Ш^1(\mathscr{D}, h)$, all $u \in \mathrm{Gal}(\Omega/E)_{\ell,\infty}$ and all $u' \in H_{\ell,\infty}$ with $u' = \iota_{E/F}^{\Omega}(u)$.

LEAN `Tower.IsDesc`

Proof of Theorem A. Inputs R1 and R2 are used for the number field E with its algebraic closure Ω, for the datum $\mathscr{D}$ and the integer h; their hypotheses are among those of the theorem. By Proposition 5.2(a) and Definition 2.5, the map $\iota_{E/F}^{\Omega}(\cdot)$ carries $\mathrm{Gal}(\Omega/E)_{\ell,\infty}$ bijectively onto $\mathrm{Gal}_F(\Omega/E)_{\ell,\infty}$, and this is $H_{\ell,\infty}$ by hypothesis. By Proposition 7.4, in the case described after it, composition with this map is an isomorphism from $D_\infty(\ell, \ell, H)$ onto the module $D_\infty(\ell, \ell, \mathrm{Gal}(\Omega/E))$ that is formed in $\mathrm{Gal}(\Omega/E)$.

Let $\varphi \in D_\infty(\ell, \ell, H)$ and $g \in \mathrm{Gal}_F(\Omega/E)$. The equation $T_{\ell,\ell,H;h}(g)\,\varphi = \varphi$ says that

$$\kappa_\ell^{\Omega/F}(g)^{-h}\,\varphi(g^{-1}ug) = \varphi(u) \qquad \text{for all } u \in H_{\ell,\infty}.$$

The group $H_{\ell,\infty}$ is normal in $\mathrm{Gal}(\Omega/F)$, so we may write $u = gwg^{-1}$ with $w \in H_{\ell,\infty}$, and the equation becomes

$$\varphi(gwg^{-1}) = \kappa_\ell^{\Omega/F}(g)^{-h}\,\varphi(w) \qquad \text{for all } w \in H_{\ell,\infty}.$$

So the isomorphism above carries the module of invariants onto the module of Input R2 for the field E:

$$D_\infty(\ell, \ell, H)(-h)^{\mathrm{Gal}_F(\Omega/E)} \longrightarrow \mathscr{C}_\ell(\mathrm{Gal}(\Omega/E)_{\ell,\infty}; \mathcal{Q}_\ell^{\Omega/E}(-h)).$$

By Input R2 the map $\xi \mapsto \mathrm{res}_\infty(\mathscr{D}, h; \xi)$ sends $Ш^1(\mathscr{D}, h)$ onto the second module, and by Input R1 it is injective. It is $\mathbb{Z}_\ell$-linear. Composed with the inverse of the isomorphism above it is the map Φ of the theorem, and it is given by restriction for E, $\mathscr{D}$, h and H by construction. □

LEAN `Tower.desc`

9 A separation lemma

The unit contains one more statement, used in the lemma on characters of the first note [N1, §8] to show that the characters of a $\mathbb{Z}_\ell$-module separate its elements. For a prime number ℓ we write $v_\ell(s)$ for the ℓ-adic valuation of an element s of $\mathbb{Z}_\ell$.

Lemma 9.1. *Let ℓ be a prime number, M a $\mathbb{Z}_\ell$-module and $b \in M$ a nonzero element. Then there is a nonzero $y \in \mathbb{Q}_\ell/\mathbb{Z}_\ell$ such that every $s \in \mathbb{Z}_\ell$ with $sb = 0$ satisfies $sy = 0$.*

Proof. A nonzero $s \in \mathbb{Z}_\ell$ is the product of $\ell^{v_\ell(s)}$ and a unit, so it kills an element of a module if and only if $\ell^{v_\ell(s)}$ does. Suppose first that some power of ℓ kills b, and let ℓ^r be the smallest one. Then $r \geq 1$, because $b \neq 0$. Let y be the class of ℓ^{-r} in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$; it is nonzero and $\ell^r y = 0$. If $s \neq 0$ and $sb = 0$, then $\ell^{v_\ell(s)} b = 0$, so $v_\ell(s) \geq r$, so $\ell^{v_\ell(s)} y = 0$ and $sy = 0$. If no power of ℓ kills b, then only $s = 0$ kills b, and the class of ℓ^{-1} will do. □

LEAN `exists_qz_ne_zero_annihilators_of_ne_zero`; the classes of ℓ^{-r} come from `Kum.zmodToQZ`

In [N1] the lemma is applied as follows: $sb \mapsto sy$ is a well-defined homomorphism from the submodule generated by b to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$, and it extends to M because $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is a divisible group.

10 Where the theorems are used

In [N1, §8] the base field is called L and the intermediate field F; they are the fields F and E of this note. Input 2a there is Theorem A for $H = \mathrm{Gal}(\Omega/F)$, and Input 2b is Theorem B for $H = \mathrm{Gal}(\Omega/F)$, with the element η there in the place of γ. With them the first note computes the length of the group $Ш^1(\mathscr{D}, h)$ of a datum $\mathscr{D}$ for the layer $E = F\big(\mu_{\ell^{a_\ell(F)+m}}(\Omega)\big)$ of index m as the length of the kernel of $T_{\ell,\ell,\mathrm{Gal}(\Omega/F);h}(\eta) - 1$ on $D_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))(-h)$, where η is a power of an ℓ-generator for $\mathrm{Gal}(\Omega/F)$, and by duality as the length of a cokernel on $X_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))(h)$. Proposition 3.3 and Proposition 5.2 enter the description of the layers there, the lemmas on roots of unity and on the layers [N1, §8], and the tower condition of Definition 2.12 is the hypothesis of its main theorem. With this note, of the three inputs of [N1] the first is proved in [N2]; the second is reduced to Inputs G, R1 and R2 and to the comparison of two descriptions of the length of the group of locally trivial classes that is cited there; the third, on global duality, has not been read yet.

11 Notes on the formal text

1. *Theorem A is an assembly.* Its formal proof transports the characters from $\mathrm{Gal}(\Omega/F)$ to $\mathrm{Gal}(\Omega/E)$, rewrites the invariance as the equation of Input R2, and applies the two theorems on restriction. The hypotheses $h \neq 0$ and condition $\mathrm{P}_\ell(\Omega/E)$ are used in those two theorems only.
2. *The form of Theorem A.* The theorem is stated as in the archive: there is an isomorphism Φ from $Ш^1(\mathscr{D}, h)$ to the module of invariants such that $(\Phi\xi)(u')$ is the value of $\mathrm{res}_\infty(\mathscr{D}, h; \xi)$ at u, whenever $u' \in H_{\ell,\infty}$ is the element u of $\mathrm{Gal}(\Omega/E)_{\ell,\infty}$ regarded in $\mathrm{Gal}(\Omega/F)$. Every element of $H_{\ell,\infty}$ arises so from exactly one u, hence Φ is the restriction map, as is said after the theorem.
3. *Two algebraic closures.* Proposition 7.4 is stated for two fields with two algebraic closures and an isomorphism between them. The archive uses it once, with the identity.
4. *Where the hypotheses of Theorem B enter.* Closedness and normality of H are used for the integers n and r. The group V need not be closed or normal, and γ need not generate it in any other sense than Definition 2.10.
5. *The integer $a_\ell(F)$* is defined in the archive as the supremum of a set of natural numbers, which is meaningful because of Lemma 3.2. The definition is made there for every field and every natural number in the place of the prime.
6. *Lemma 7.3* is proved in the archive in one direction, and the other direction is obtained where it is needed by exchanging the two fields. The equivalence is stated here at once.

7. *Facts from other units.* The properties of the map θ in Lemma 7.2 and of the group $\mathrm{Gal}_F(\Omega/E)$ in Proposition 5.2(a) are theorems of other units of the archive. Their formal proofs were not read; the short arguments given here are the standard ones.
8. *The tower condition* is stated in the archive for the module over the algebraic closure of F that the library constructs, not over a closure that is given. The modules over two algebraic closures of F are isomorphic (Proposition 7.4, for an isomorphism of the two closures over F).
9. *The unit.* The 39 declarations treated here are those of the unit that the final theorems use. The files of the unit contain further declarations, on norms of ideal classes, on coinvariants and on eigenspaces, that the final theorems do not use; for a few of them the reading project could not decide this.

How this note was written. The reading project supplied a dossier of the unit: the statements, a glossary, readings of the imported declarations, and a structured proof of every theorem in which each step quotes the lines of the archive that it renders. A program compared the quotations with the archive, for all 213 steps of the 21 proofs. The proofs of this note were written from those structured proofs. The formal statements of the theorems and the file of definitions were read in the archive and compared with the statements above; of the formal proofs, the opening lines of the proof of Theorem B were read, to identify the two results it cites. The arguments for Lemma 3.1 and Lemma 7.3 are shorter here than in the archive and are ours.

Changes in this edition. The earlier version of this note fixed the prime, the number field and its algebraic closure once and then wrote the modules, the groups, the characters and the operators without them: a bare letter with the subscript ∞ for the modules $D_\infty(\ell, N, H)$ and $X_\infty(\ell, N, H)$, a subscript for the levels $H_{\ell,n}$, one letter each for the cyclotomic character, the exponent $a_\ell(F)$ and the operators $T_{\ell,N,H;h}(g)$, and the group of locally trivial classes without its datum. Definitions stood in running text, and hypotheses in sentences before the statements. Now every function that the archive defines is written with all the arguments of its formal definition, the definitions are numbered, and every statement states its hypotheses or cites the Setting that holds them. Three things changed beyond notation. Theorem A is stated in the form of the archive, with the isomorphism Φ and Definition 8.3; its earlier form, that restriction is an isomorphism onto the invariants, is the paragraph after it. The cohomology classes and Inputs R1 and R2 are stated for the field of Setting 2.1, as in the archive, and applied to E in the proof of Theorem A. The tower condition (Definition 2.12) names the algebraic closure over which its module is formed, which the earlier text left out. No proof changed in content.

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 first 39 rows are the declarations of the unit.

In this note	Lean declaration	File	Lines
Def. 2.7	`Tower.dRep`	XTwApplyApply.lean	41–43
Def. 2.7	`Tower.xRep`	XTwApplyApply.lean	45–46
Def. 2.7	`Tower.xRep_apply`	XTwApplyApply.lean	48–48

In this note	Lean declaration	File	Lines
Def. 2.8	`Tower.twist`	XTwApplyApply.lean	50–54
Def. 2.8	`Tower.dTw`	XTwApplyApply.lean	56–56
Def. 2.8	`Tower.xTw`	XTwApplyApply.lean	58–58
Def. 2.8	`Tower.dTw_apply`	XTwApplyApply.lean	60–61
Def. 2.8	`Tower.xTw_apply`	XTwApplyApply.lean	63–64
Lemma 2.9	`Tower.xTw_apply_apply`	XTwApplyApply.lean	66–69
Def. 2.8	`Tower.ShaD`	XTwApplyApply.lean	73–74
Def. 2.10	`Tower.IsGen`	XTwApplyApply.lean	36–37
Def. 2.11	`Tower.cZero`	XTwApplyApply.lean	104–104
Def. 2.11	`Tower.layU`	XTwApplyApply.lean	108–108
Def. 2.11	`Tower.layF`	XTwApplyApply.lean	110–110
Def. 2.6	`Tower.XN`	XTwApplyApply.lean	112–112
Def. 2.6	`Tower.XX`	XTwApplyApply.lean	114–114
Def. 2.6	`Tower.XP`	XTwApplyApply.lean	116–116
Def. 2.12	`Tower.GenLE`	XTwApplyApply.lean	11–12
Def. 2.12	`Tower.GenLE.finite`	XTwApplyApply.lean	14–17
Def. 2.12	`Tower.cokerLen`	XTwApplyApply.lean	24–25
Def. 2.12	`Tower.xRank`	XTwApplyApply.lean	34–34
Def. 2.12	`Tower.IsTower`	XTwApplyApply.lean	120–124
Def. 8.3	`Tower.IsDesc`	IdealNormClassCongr.lean	99–101
Lemma 3.1	`cyc_mem_princ_iff`	CycMemPrincIff.lean	7–34
Lemma 3.2	`le_finrank`	CycMemPrincIff.lean	36–49
Prop. 3.3(a)	`ex_iff`	CycMemPrincIff.lean	51–59
Prop. 3.3(a)	`all_iff`	CycMemPrincIff.lean	61–79
Prop. 3.3	`Tower.muQ`	CycMemPrincIff.lean	81–104
Prop. 4.1	`Tower.dinfTors`	DinfTors.lean	7–86
Prop. 5.1	`Tower.existsGen`	ExistsGen.lean	9–28
Prop. 5.2	`Tower.genGal`	GenGal.lean	9–33
Theorem B	`Tower.shaDGen`	ShaDGen.lean	9–59
Lemma 7.3(a)	`dt_val_lt_one`	DinfTransport.lean	8–12
Lemma 7.3(b)	`dt_dec`	DinfTransport.lean	14–25
Lemma 7.3(b)	`dt_ine`	DinfTransport.lean	27–34
Prop. 7.4, proof	`dt_mem`	DinfTransport.lean	36–48
Prop. 7.4	`Tower.dinfTransport`	DinfTransport.lean	50–76
Theorem A	`Tower.desc`	Imports.lean	10–147
Lemma 9.1	`exists_qz_ne_zero_annihilators_of_ne_zero`	QzSep.lean	8–45
Def. 2.2	`G`	Statement.lean	6–6
Def. 2.2	`QZ`	Statement.lean	15–15
Def. 8.1	`LData`	Statement.lean	54–63
Def. 8.1	`qzTw`	Statement.lean	67–69
Def. 8.1	`Sha`	Statement.lean	75–76
Def. 2.2	`Gal.cycZ`	Global.lean	90–92
Def. 2.3	`princ`	LeNuIffPowMemPrinc.lean	16–16
Def. 2.3	`Base.levU`	ConjStableShaFam.lean	187–187
Def. 2.3	`Base.cycU`	ConjStableShaFam.lean	189–189
Def. 2.3	`Base.qExp`	ConjStableShaFam.lean	193–193
Def. 2.3	`Base.gamU`	ConjStableShaFam.lean	195–195
Def. 2.5	`Base.galOf`	ConjStableShaFam.lean	43–47
Def. 2.5	`Base.galEmb`	ConjStableShaFam.lean	65–65
Prop. 5.2, proof	`Base.galEmbFam`	GalEmbFam.lean	5–30
Prop. 5.2, proof	`Base.galEmbTop`	GalEmbTop.lean	32–69
Def. 2.6	`Kum.Dinf`	Mk0IdMapCongr.lean	195–195
Def. 2.6	`Kum.Xinf`	Mk0IdMapCongr.lean	197–197
Def. 2.7	`Kum.funRep`	Mk0IdMapCongr.lean	121–124
Def. 8.2	`Kum.EqHom`	Mk0IdMapCongr.lean	109–110

In this note	Lean declaration	File	Lines
Def. 2.3	`Kum.Un`	Mk0IdMapCongr.lean	186–186
Def. 2.3	`Kum.Procyc`	Mk0IdMapCongr.lean	191–191
Def. 8.1	`Kum.resInf`	Mk0IdMapCongr.lean	214–217
Def. 2.7	`Kum.funRepMem`	FunRepMem.lean	5–46
Theorem B, proof	`Kum.dinfNil`	DinfNil.lean	62–235
Input G	`Kum.existsGen`	ExistsGen.lean	32–96
Input R1	`Kum.resInfInj`	ResInfInj.lean	58–171
Input R2	`Kum.resInfOnto`	ResInfOnto.lean	102–166
Lemma 9.1, proof	`Kum.zmodToQZ`	ZmodToQZ.lean	5–78
Def. 2.12	`HasMuQ`	LemmaK.lean	9–9
Def. 8.1	`qzG`	LevelInertiaLeLevelDec.lean	22–22
Lemma 7.2	`galTransport`	GalTransport.lean	7–71

Three statements as they are written in the archive. Theorem A; here `k` and `L` are the fields F and E, `U` is the group H, `galOf k L Ω` is $\mathrm{Gal}_F(\Omega/E)$, `e` is h, `D` is the datum $\mathscr{D}$, and `Procyc L Ω l` is condition $\mathrm{P}_\ell(\Omega/E)$:

```
theorem UpperTheory.V.Tower.desc :
    ∀ (k L Ω : Type) [Field k] [NumberField k] [Field L] [NumberField L] [Field Ω] [Algebra k L] [Algebra k Ω]
      [Algebra L Ω] [IsScalarTower k L Ω] [IsAlgClosure k Ω] [IsAlgClosure L Ω] (l : ℕ) [Fact l.Prime] (D :
      LData L Ω l) (e : ℤ) (U : Subgroup (G k Ω)) [U.Normal], e ≠ 0 → Procyc L Ω l → cycU l U = cycU l (galOf k
      L Ω) →
      ∃ Φ : Sha D e ≃ₗ[ℤ_[l]] ShaD l l U (galOf k L Ω) e, IsDesc L D e U Φ.toLinearMap
```

Theorem B; here `dTw l N U e γ` is the operator $T_{\ell,N,H;h}(\gamma)$:

```
theorem UpperTheory.V.Tower.shaDGen :
    ∀ (k Ω : Type) [Field k] [NumberField k] [Field Ω] [Algebra k Ω] [IsAlgClosure k Ω] (l : ℕ) [Fact l.Prime] (N
      : ℕ) (U V : Subgroup (G k Ω)) [U.Normal] (e : ℤ) (γ : G k Ω), IsClosed (U : Set (G k Ω)) → V ≤ U → IsGen
      l V γ →
      ShaD l N U V e = LinearMap.ker (dTw l N U e γ - 1) ∧ ShaD l N U V e = LinearMap.ker (dTw l N U e γ⁻¹ - 1)
```

Proposition 3.3; here `cZero l L` is the integer $a_\ell(F)$ of the field, which the archive calls `L`, `Un L Ω l c` is the group $\mathrm{Gal}(\Omega/F)_{\ell,c}$ and `qExp l` is q_ℓ:

```
theorem UpperTheory.V.Tower.muQ :
    ∀ (L Ω : Type) [Field L] [NumberField L] [Field Ω] [Algebra L Ω] [IsAlgClosure L Ω] (l : ℕ) [Fact l.Prime],
      (∀ c : ℕ, (∃ ζ : L, IsPrimitiveRoot ζ (l ^ c)) ↔ c ≤ cZero l L) ∧ (∀ c : ℕ, Un L Ω l c = ⊤ ↔ c ≤ cZero l
      L) ∧
      (HasMuQ l L ↔ qExp l ≤ cZero l L) ∧ (HasMuQ l L → IsTotallyComplex L ∧ Procyc L Ω l) ∧ (Procyc L Ω l ↔ l
        ≠ 2 ∨ HasMuQ l L)
```

Notation

The symbols of the text. In brackets: the function of the archive with its arguments, or the name that the archive uses.

ℓ, $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$ a prime [`l`]; the ℓ-adic integers and numbers

$\mathbb{Q}_\ell/\mathbb{Z}_\ell$ the quotient group of $\mathbb{Q}_\ell$ by $\mathbb{Z}_\ell$ [`QZ l`]

F, Ω, $\mathrm{Gal}(\Omega/F)$ a number field [`k`, `F`, `L`]; an algebraic closure; the automorphisms of Ω over F [`G F Ω`]

$\kappa_\ell^{\Omega/F}(g)$ the ℓ-adic cyclotomic character of Ω over F at g [`cycZ F Ω l g`]

$U_\ell^{(n)}$, W the units congruent to 1 modulo ℓ^n [`princ l n`]; a closed subgroup of $\mathbb{Z}_\ell^\times$

H, $H_{\ell,n}$, $H_{\ell,\infty}$ a subgroup of $\mathrm{Gal}(\Omega/F)$ [`U`]; its elements with cyclotomic value in $U_\ell^{(n)}$ [`levU l U n`]; those with value 1 [`cycU l U`]

$\mathrm{Gal}(\Omega/F)_{\ell,n}$ the same for the whole group [`Un F Ω l n`]

q_ℓ, H_{ℓ,q_ℓ} 2 for $\ell = 2$, else 1 [`qExp l`]; the subgroup of H of that level [`gamU l U`]

$\mathrm{P}_\ell(\Omega/F)$ the condition of Definition 2.3(iv) [`Procyc F Ω l`]

E, $\mathrm{Gal}_F(\Omega/E)$ a finite extension of F in Ω; the elements of $\mathrm{Gal}(\Omega/F)$ that fix E [`galOf k E Ω`]

$\iota^{\Omega}_{E/F}(g)$ an element g of $\mathrm{Gal}(\Omega/E)$ regarded in $\mathrm{Gal}(\Omega/F)$ [`galEmb k E Ω g`]

ζ, t, $\mu_{\ell^n}(\Omega)$ a root of unity; an element of Ω; the t with $t^{\ell^n}=1$

A, $\mathfrak{m}_A$ a valuation ring of Ω; its maximal ideal

G_A, I_A decomposition and inertia group of A in $\mathrm{Gal}(\Omega/F)$ [`Dec A`, `Ine A`]

C, N, Λ, M a subgroup of $\mathrm{Gal}(\Omega/F)$; an integer ≥ 0; a ring; a module over it

$D_N(C;\Lambda,M)$ the characters $C\to M$ with the conditions of Definition 2.6 [`XDual N U R M`]

$D_\infty(\ell,N,H)$, $X_\infty(\ell,N,H)$ $D_N(H_{\ell,\infty};\mathbb{Z}_\ell,\mathbb{Q}_\ell/\mathbb{Z}_\ell)$ [`Dinf l N U`]; its dual [`Xinf l N U`]

$X_\infty(\ell,N,\mathrm{Gal}(\Omega/F))$ the dual for the whole group [`XN l L Ω N`]

$\overline{F}$, $X_\infty(\ell,1,\mathrm{Gal}(\overline{F}/F))$, $X_\infty(\ell,\ell,\mathrm{Gal}(\overline{F}/F))$ the algebraic closure of the library; the duals over it with $N=1$ [`XX l L`] and $N=\ell$ [`XP l L`]

φ, ψ, χ characters; an element of $X_\infty(\ell,N,H)$

g, γ, u, u', w elements of groups; γ an ℓ-generator (Definition 2.10) [`IsGen l U γ`]

Γ, π, ω, $\pi\otimes\omega$ a group; a representation; a homomorphism to the units of the ring; the twist of π by ω [`twist π ψ`]

$\mathscr{F}_\Lambda(C,M)$ conjugation on the maps $C\to M$ [`funRep R M U`]

$\rho_{\ell,N,H}$, $\rho^\vee_{\ell,N,H}$ conjugation on $D_\infty(\ell,N,H)$ [`dRep l N U`]; the dual action [`xRep l N U`]

h, $T_{\ell,N,H;h}$, $T^\vee_{\ell,N,H;h}$ an integer [`e`]; the twisted actions (Definition 2.8) [`dTw l N U e`, `xTw l N U e`]

$D_\infty(\ell,N,H)(-h)$, $X_\infty(\ell,N,H)(h)$ the two modules with these actions

V, $D_\infty(\ell,N,H)(-h)^V$ a subgroup of $\mathrm{Gal}(\Omega/F)$; the elements fixed by all $T_{\ell,N,H;h}(g)$, $g\in V$ [`ShaD l N U V e`]

$a_\ell(F)$, a the largest c with a root of unity of order ℓ^c in F [`cZero l L`]; this number in a proof

$F\big(\mu_{\ell^{a_\ell(F)+m}}(\Omega)\big)$ the layer of index m [`layF l L Ω m`]

$\mathrm{Gal}(\Omega/F)_{\ell,a_\ell(F)+m}$ its group [`layU l L Ω m`]

$\mathrm{len}\,M$, α the length of a module; a linear map $M\to M$

$\mathrm{len}\,D_\infty(\ell,N,H)[\ell]$ the length of the elements killed by ℓ [`xRank l N U`]

R the number of generators in the tower condition

n, m, r, c, j integers

s, $v_\ell(s)$ an element of $\mathbb{Z}_\ell$ or of $\mathbb{Q}_\ell$; its ℓ-adic valuation [`vl l x`]

F', Ω', H', A', g' a second number field with its algebraic closure, a subgroup, a valuation ring, an element

f, τ, θ a homomorphism $F\to F'$; an isomorphism $\Omega\to\Omega'$; the map $g'\mapsto\tau^{-1}g'\tau$

S, $\mathfrak{p}$, $G_S(\Omega)$ the primes of F above ℓ; one of them; the Galois group of the largest extension unramified outside S

$\mathrm{Dat}_\ell(\Omega/F)$, $\mathscr{D}$ the data of Definition 8.1 [`LData F Ω l`]; one of them, with its valuation rings $A_\mathfrak{p}$ and its homomorphism χ

$\mathscr{Q}(\mathscr{D})(-h)$ $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ with the action through χ^{-h} [`qzTw D e`]

$H^1(\mathscr{Q}(\mathscr{D})(-h))$ its first cohomology group

z, ξ, y a crossed homomorphism; its class; an element of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$

$Ш^1(\mathscr{D},h)$ the locally trivial classes [`Sha D e`]

$\mathrm{res}_\infty(\mathscr{D},h;\xi)$ the restriction of the class ξ (Definition 8.1) [`resInf D e ξ`]

$\mathscr{Q}_\ell^{\Omega/F}(-h)$ $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ with the action of $\mathrm{Gal}(\Omega/F)$ through $\kappa_\ell^{\Omega/F}(\cdot)^{-h}$ [`qzG F Ω l e`]

$\mathscr{E}_N(C;\pi)$ the equivariant characters of Definition 8.2 [`EqHom N U ρ`]

b a nonzero element of a $\mathbb{Z}_\ell$-module (Lemma 9.1)

Φ, T the isomorphism of Theorem A; in the summary, a twisted action

L, η the base field and the generator in the first note

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`.

[N1] *Twisted cokernels in a cyclotomic tower*, Deformalization 1, riemann-rev, `digests/tower-bound.pdf`.

[N2] *Local nilpotence over a cyclotomic tower*, Deformalization 2, riemann-rev, `digests/local-nilpotence.pdf`.

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

[Se] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer, 1973.

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