DEFORMALIZATION 2

Local nilpotence over a cyclotomic tower

One part of a 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, let ℓ be a prime, and let $\kappa_\ell^{\Omega/F}(\cdot)$ be the ℓ-adic cyclotomic character of the Galois group $\mathrm{Gal}(\Omega/F)$. This group acts by conjugation on the characters of the kernel of the cyclotomic character, with values in $\mathbb{Q}_\ell/\mathbb{Z}_\ell$. We show that every locally constant character φ is fixed by all g with $\kappa_\ell^{\Omega/F}(g) \equiv 1$ modulo ℓ^n, for some n, and that for every γ with $\kappa_\ell^{\Omega/F}(\gamma) \equiv 1$ modulo ℓ a power of the operator "action of γ, minus the identity" kills φ; the exponent $\ell^n k_0$ suffices, where ℓ^{k_0} kills φ. This is the *local nilpotence* that the first note of this series [N1] used as an input. By duality it makes the action of γ unipotent modulo ℓ on the Iwasawa module. The proof is a compactness argument in the profinite group $\mathrm{Gal}(\Omega/F)$ and one congruence between polynomials.

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 part of one unit, on Kummer theory: 13 of its 144 declarations, those that define the modules of characters and prove local nilpotence. The other 131 belong to notes to come (§6). Everything stated in §§1–4 is proved in full; §5 states the two results of the archive that use the theorem, one derived here from a proposition of the first note, the other quoted without proof. Every statement was compared with its formal counterpart at commit `40e56bab` of the public mirror; Appendix A is the concordance of 27 declarations. The note was written from the structured proofs of the reading project, without opening the Lean files of the unit (§6).

1 The statement

In the first note [N1] the lengths of certain groups of Galois cohomology along the cyclotomic tower of a number field F were expressed through one operator on one module, the Iwasawa module $X_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))$ of a prime ℓ and an algebraic closure Ω of F, and the estimates needed that this operator is unipotent modulo ℓ. This module is the dual of a discrete module $D_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))$ of characters, and on a discrete module unipotence takes the form proved here: every element is killed by a power of the operator minus the identity. The first note stated this as its Input 1, with a sketch. This note proves it, in the generality of the archive: there the second argument of the two modules is any integer $N \geq 0$, and the third is any closed normal subgroup of $\mathrm{Gal}(\Omega/F)$. The notation is set up in §2.

Theorem A (local nilpotence). *Let ℓ be a prime number, F a number field and Ω an algebraic closure of F. Let H be a closed normal subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ be an integer, and let φ be an element of the module $D_\infty(\ell, N, H)$ of characters of $H_{\ell,\infty}$. Write*

$$\pi = \mathscr{F}_{\mathbb{Z}_\ell}(H_{\ell,\infty}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$$

for the representation of $\mathrm{Gal}(\Omega/F)$ by conjugation on the functions from $H_{\ell,\infty}$ to $\mathbb{Q}_\ell/\mathbb{Z}_\ell$.

(i) *There is an integer $n \geq 0$ such that $\pi(g)\varphi = \varphi$ for every $g \in H_{\ell,n}$.*

(ii) *Some power of ℓ kills φ. If $\ell^{k_0}\varphi = 0$ and n is as in* (i)*, then for every $\gamma \in H_{\ell,1}$ and $k = \ell^n k_0$*

$$(\pi(\gamma) - 1)^k \varphi = 0 \qquad \text{and} \qquad \ell^k \varphi = 0.$$

LEAN `Kum.dinfNil`

Here $\mathrm{Gal}(\Omega/F)$ is the Galois group of Ω over F with its usual topology, $\kappa_\ell^{\Omega/F}(g)$ is the value at g of its ℓ-adic cyclotomic character, $H_{\ell,n}$ is the group of all $g \in H$ with $\kappa_\ell^{\Omega/F}(g) \equiv 1$ modulo ℓ^n, and $H_{\ell,\infty}$ is the group of all $g \in H$ with $\kappa_\ell^{\Omega/F}(g) = 1$. The group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the quotient of the ℓ-adic numbers by the ℓ-adic integers, the module $D_\infty(\ell, N, H)$ is that of Definition 2.3, and $\pi(g)\varphi$ is the character $x \mapsto \varphi(g^{-1}xg)$. The archive states (ii) in this form: for every γ there is an exponent k with the two properties. Its proof gives the value above, the same for all γ.

2 Characters and conjugation

Conventions. In the definitions of this note ℓ is a prime number, $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers and $\mathbb{Q}_\ell$ its field of fractions; F is a number field, and Ω is an algebraic closure of F. A notation shows the prime and the two fields exactly where the formal definition has them as written arguments; elsewhere they are understood. A theorem names them again in its own statement.

Definition 2.1 (the Galois group, the coefficients, the cyclotomic character). The *Galois group* $\mathrm{Gal}(\Omega/F)$ is the group of the automorphisms of the field Ω that fix every element of F. It carries its usual topology: the subgroups $\mathrm{Gal}(\Omega/E)$, for E a finite extension of F in Ω, are a basis of neighbourhoods of 1.

The group $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the quotient of the additive group of $\mathbb{Q}_\ell$ by $\mathbb{Z}_\ell$. It is a module over $\mathbb{Z}_\ell$.

The *ℓ-adic cyclotomic character* of Ω over F is the homomorphism $g \mapsto \kappa_\ell^{\Omega/F}(g)$ from $\mathrm{Gal}(\Omega/F)$ to the group $\mathbb{Z}_\ell^\times$ of units of $\mathbb{Z}_\ell$ such that $g(\zeta) = \zeta^{\kappa_\ell^{\Omega/F}(g)}$ for every $g \in \mathrm{Gal}(\Omega/F)$ and every root of unity ζ of ℓ-power order in Ω. It is continuous.

LEAN `G · QZ · Gal.cycZ`

The group $\mathrm{Gal}(\Omega/F)$ is profinite: it is compact, and every neighbourhood of 1 contains an open normal subgroup [NSW, Ch. I, §1].

Definition 2.2 (the groups). For an integer $n \geq 1$ let $U_\ell^{(n)} = 1 + \ell^n\mathbb{Z}_\ell$, and let $U_\ell^{(0)} = \mathbb{Z}_\ell^\times$; these are open subgroups of $\mathbb{Z}_\ell^\times$. For a subgroup H of $\mathrm{Gal}(\Omega/F)$ and an integer $n \geq 0$ put

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

For the whole group we also write $\mathrm{Gal}(\Omega/F)_{\ell,n}$ for the group of all $g \in \mathrm{Gal}(\Omega/F)$ with $\kappa_\ell^{\Omega/F}(g) \in U_\ell^{(n)}$; it is the first of the two groups for $H = \mathrm{Gal}(\Omega/F)$.

LEAN princ · Base.levU · Base.cycU · Kum.Un

So $H_{\ell,0} = H$, the groups $H_{\ell,n}$ decrease as n grows, and $H_{\ell,\infty}$, the intersection of H with the kernel of the cyclotomic character, is their intersection. If H is normal in $\mathrm{Gal}(\Omega/F)$, so are all of these. The group $\mathrm{Gal}(\Omega/F)_{\ell,n}$ is the Galois group of Ω over the field generated over F by the roots of unity of order ℓ^n, and $\mathrm{Gal}(\Omega/F)_{\ell,\infty}$ is that of Ω over the field F_∞ generated by all roots of unity of ℓ-power order.

Definition 2.3 (characters). A *valuation ring* of Ω is a subring A such that $z \in A$ or $z^{-1} \in A$ for every non-zero $z \in \Omega$; its maximal ideal $\mathfrak{m}_A$ consists of the non-units of A. The *decomposition group* G_A is the group of all $g \in \mathrm{Gal}(\Omega/F)$ with $g(A) = A$, and the *inertia group* I_A is the subgroup of those that act trivially on the residue field $A/\mathfrak{m}_A$.

Let C be a subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ be an integer, and let M be a module over a commutative ring R. The module $D_N(C; R, M)$ consists of the homomorphisms $\varphi : C \to M$ that are locally constant, 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 $N \in \mathfrak{m}_A$. It is an R-module under pointwise operations. For a subgroup H of $\mathrm{Gal}(\Omega/F)$ put

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

LEAN Gal.Dec · Gal.Ine · Kum.XDual · Kum.Dinf · Kum.Xinf

The elements of $D_N(C; R, M)$ are the characters of C that are unramified at every place of Ω and trivial on the decomposition groups of the places above the primes that divide N. For $H = \mathrm{Gal}(\Omega/F)$ and $N = \ell$ the modules $D_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))$ and $X_\infty(\ell, \ell, \mathrm{Gal}(\Omega/F))$ are those of the first note [N1, §7], with $L = F$.

Definition 2.4 (conjugation). Let C be a normal subgroup of $\mathrm{Gal}(\Omega/F)$ and $g \in \mathrm{Gal}(\Omega/F)$. *Conjugation* by g is the homomorphism from C to C that sends $x \in C$ to $g^{-1}xg$. Let M be a module over a commutative ring R. We write $\mathscr{F}_R(C, M)$ for the following representation of the group $\mathrm{Gal}(\Omega/F)$ on the R-module of all functions $C \to M$: the element g sends a function φ to the function $\mathscr{F}_R(C, M)(g)\varphi$ with

$$\big(\mathscr{F}_R(C, M)(g)\varphi\big)(x) = \varphi(g^{-1}xg) \qquad (x \in C).$$

Each $\mathscr{F}_R(C, M)(g)$ is R-linear, and for all $g, h \in \mathrm{Gal}(\Omega/F)$

$$\mathscr{F}_R(C, M)(gh) = \mathscr{F}_R(C, M)(g)\,\mathscr{F}_R(C, M)(h).$$

LEAN Base.conjHom · Kum.funRep

The archive defines conjugation for a normal subgroup of any group; only the group $\mathrm{Gal}(\Omega/F)$ occurs in this note.

Definition 2.5 (equivariant characters). Let C be a subgroup of $\mathrm{Gal}(\Omega/F)$ and let M be a module over a commutative ring R. For an automorphism σ of the field Ω and an R-linear map $\theta : M \to M$, the module $\mathscr{C}(C; \sigma, \theta)$ consists of the functions $\varphi : C \to M$ such that

$$\varphi(x') = \theta\big(\varphi(x)\big) \qquad \text{for all } x, x' \in C \text{ with } x' \circ \sigma = \sigma \circ x.$$

It is an R-module under pointwise operations. For an integer $N \geq 0$ and a representation ρ of $\mathrm{Gal}(\Omega/F)$ on M by R-linear maps put

$$\mathscr{E}_N(C;\rho) = D_N(C;R,M) \cap \bigcap_{g\in\mathrm{Gal}(\Omega/F)} \mathscr{C}(C;g,\rho(g)).$$

LEAN `Kum.conjCond` · `Kum.EqHom`

For an element g of $\mathrm{Gal}(\Omega/F)$ in the place of σ, the relation $x' \circ g = g \circ x$ says that $x' = gxg^{-1}$. So a function φ lies in $\mathscr{E}_N(C;\rho)$ if and only if it lies in $D_N(C;R,M)$ and

$$\varphi(gxg^{-1}) = \rho(g)\varphi(x) \qquad \text{for all } g \in \mathrm{Gal}(\Omega/F) \text{ and all } x \in C \text{ with } gxg^{-1} \in C.$$

Proposition 2.6. *Let F be a number field and Ω an algebraic closure of F. Let C be a normal subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ be an integer, and let M be a module over a commutative ring R.*

(a) *If $\varphi \in D_N(C;R,M)$ and $g \in \mathrm{Gal}(\Omega/F)$, then $\mathscr{F}_R(C,M)(g)\varphi \in D_N(C;R,M)$.*

(b) *If $\varphi \in D_N(C;R,M)$ and $g \in C$, then $\mathscr{F}_R(C,M)(g)\varphi = \varphi$.*

(c) *Let ρ be a representation of $\mathrm{Gal}(\Omega/F)$ on M by R-linear maps. A function $\varphi : C \to M$ lies in $\mathscr{E}_N(C;\rho)$ if and only if it lies in $D_N(C;R,M)$ and $\rho(g)\big((\mathscr{F}_R(C,M)(g)\varphi)(x)\big) = \varphi(x)$ for all $g \in \mathrm{Gal}(\Omega/F)$ and $x \in C$.*

Proof. (a) The map $x \mapsto g^{-1}xg$ is a continuous homomorphism of C to itself, so $\mathscr{F}_R(C,M)(g)\varphi$ is a locally constant homomorphism. Let A be a valuation ring of Ω. Then $g^{-1}(A)$ is a valuation ring with maximal ideal $g^{-1}(\mathfrak{m}_A)$, and

$$g^{-1}G_A g = G_{g^{-1}(A)}, \qquad g^{-1}I_A g = I_{g^{-1}(A)}.$$

So for $x \in C \cap I_A$ the element $g^{-1}xg$ lies in $C \cap I_{g^{-1}(A)}$, where φ vanishes. If $N \in \mathfrak{m}_A$, then $N = g^{-1}(N)$ lies in $g^{-1}(\mathfrak{m}_A)$, and the same argument applies to the decomposition groups.

(b) For $g \in C$ the three factors of $g^{-1}xg$ lie in C, and $\varphi(g^{-1}xg) = -\varphi(g) + \varphi(x) + \varphi(g) = \varphi(x)$, because M is commutative.

(c) As C is normal, the condition displayed after Definition 2.5 is a condition for all $g \in \mathrm{Gal}(\Omega/F)$ and all $x \in C$. Put $y = g^{-1}xg$. Then the condition of (c) reads $\rho(g)\varphi(y) = \varphi(gyg^{-1})$, and y runs through C when x does. □

LEAN `Kum.funRepMem`, with `conjGal_mem_Dec` and `conjGal_mem_Ine` in the proof of (a) · the module of (c): `Kum.EqHom`, defined through `Kum.conjCond`

By (a) the group $\mathrm{Gal}(\Omega/F)$ acts on $D_N(C;R,M)$, and by (b) the action factors through the quotient of $\mathrm{Gal}(\Omega/F)$ by C. For $C = H_{\ell,\infty}$, $R = \mathbb{Z}_\ell$ and $M = \mathbb{Q}_\ell/\mathbb{Z}_\ell$ this is the action on $D_\infty(\ell,N,H)$ in Theorem A, and it factors through the quotient of $\mathrm{Gal}(\Omega/F)$ by $H_{\ell,\infty}$.

3 Four facts about ℓ-adic numbers

Lemma 3.1. *Let ℓ be a prime number.*

(a) *Let $m \geq 0$ be an integer. A unit u of $\mathbb{Z}_\ell$ lies in the kernel of the reduction of units modulo ℓ^m if and only if ℓ^m divides $u-1$. So this kernel is $U_\ell^{(m)}$.*

(b) *Let $v \in \mathbb{Z}_\ell$ and $j \geq 0$. If ℓ^{j+1} divides $v-1$, then ℓ^{j+2} divides $v^\ell - 1$.*

(c) *Every element of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is killed by a power of ℓ.*

(d) *Every neighbourhood of* 1 *in* $\mathbb{Z}_\ell^\times$ *contains* $U_\ell^{(n)}$ *for some* n.

Proof. (a) The reduction of u is 1 exactly when $u-1$ lies in the kernel $\ell^m\mathbb{Z}_\ell$ of the reduction of $\mathbb{Z}_\ell$.

(b) Write $v-1=\ell^{j+1}r$ with $r\in\mathbb{Z}_\ell$, and $v^\ell-1=(v-1)\,s$ with $s=1+v+\cdots+v^{\ell-1}$. Each v^i-1 is divisible by $v-1$, so $s-\ell=\sum_{i<\ell}(v^i-1)=(v-1)\,d$ for some $d\in\mathbb{Z}_\ell$. Hence

$$v^\ell-1=\ell^{j+1}r\big(\ell+\ell^{j+1}rd\big)=\ell^{j+2}\big(r+\ell^j r^2 d\big).$$

(c) An element of $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ is the class of some $r\in\mathbb{Q}_\ell$, and $\ell^m r\in\mathbb{Z}_\ell$ for large m.

(d) The topology of $\mathbb{Z}_\ell^\times$ is induced from $\mathbb{Z}_\ell$, so a neighbourhood of 1 contains all units u with $u-1\in\ell^n\mathbb{Z}_\ell$ for some n. □

LEAN (a) `mem_princ_iff_pow_dvd_sub_one` · (b) `pow_succ_dvd_pow_prime_sub_one` · (c) `exists_prime_pow_smul_eq_zero_qz` · (d) `exists_princ_subset_of_mem_nhds_one`

By (b) and induction, an element v of $1+\ell\mathbb{Z}_\ell$ satisfies

$$v^{\ell^j}\equiv 1 \pmod{\ell^{j+1}} \qquad \text{for every } j\geq 0. \tag{1}$$

4 Proof of Theorem A

We are in the situation of Theorem A. Write $C=H_{\ell,\infty}$; then the representation of the theorem is $\pi=\mathscr{F}_{\mathbb{Z}_\ell}(C,\mathbb{Q}_\ell/\mathbb{Z}_\ell)$. The group C is a normal subgroup of $\mathrm{Gal}(\Omega/F)$, and it is closed, because H is closed and the cyclotomic character $g\mapsto\kappa_\ell^{\Omega/F}(g)$ is continuous. So C is compact. The proof uses of φ only that it is a locally constant homomorphism $C\to\mathbb{Q}_\ell/\mathbb{Z}_\ell$.

Proof of (i). The kernel of φ is an open subgroup of C, so it is the intersection of C with an open subset of $\mathrm{Gal}(\Omega/F)$ that contains 1. This subset contains an open normal subgroup W of $\mathrm{Gal}(\Omega/F)$. Thus

$$\varphi(x)=0 \qquad \text{for all } x\in W\cap C. \tag{2}$$

Every $c\in C$ *fixes* φ, that is, $\pi(c)\varphi=\varphi$. This is Proposition 2.6(b); it uses only that φ is a homomorphism.

Every $w\in W$ *fixes* φ. Let $x\in C$. The element $w^{-1}xwx^{-1}$ lies in C, because C is normal, and in W, because it is the product of w^{-1} and xwx^{-1} and W is normal. By (2),

$$(\pi(w)\varphi)(x)=\varphi\big(w^{-1}xwx^{-1}\cdot x\big)=\varphi\big(w^{-1}xwx^{-1}\big)+\varphi(x)=\varphi(x).$$

Since $\pi(ab)\varphi=\pi(a)(\pi(b)\varphi)$ for $a,b\in\mathrm{Gal}(\Omega/F)$, every element g of the set

$$S=\{wc\ :\ w\in W,\ c\in C\}$$

fixes φ: $\pi(g)\varphi=\varphi$. The set S is a union of cosets of the open subgroup W, so it is open.

Let K be the set of the elements of H that are not in S. It is closed in the compact group $\mathrm{Gal}(\Omega/F)$, hence compact, and the set $\kappa_\ell^{\Omega/F}(K)$ of the values $\kappa_\ell^{\Omega/F}(g)$, $g\in K$, is a compact, hence closed, subset of $\mathbb{Z}_\ell^\times$. It does not contain 1: an element g of H with $\kappa_\ell^{\Omega/F}(g)=1$ lies in C, and $C\subseteq S$. By Lemma 3.1(d) there is n such that $U_\ell^{(n)}$ does not meet $\kappa_\ell^{\Omega/F}(K)$. Let $g\in H_{\ell,n}$. Then $\kappa_\ell^{\Omega/F}(g)\in U_\ell^{(n)}$, so $g\notin K$; as $g\in H$, this means $g\in S$, and $\pi(g)\varphi=\varphi$.

Proof of (ii). The function φ is locally constant on a compact space, so it takes finitely many values. By Lemma 3.1(c) each of them is killed by a power of ℓ. So $\ell^{k_0}\varphi = 0$ for some $k_0 \geq 0$.

Let n be as in (i), put $q = \ell^n$, and let $\gamma \in H_{\ell,1}$. Then $\kappa_\ell^{\Omega/F}(\gamma) \in 1 + \ell\mathbb{Z}_\ell$, and by (1) with $j = n$ the unit $\kappa_\ell^{\Omega/F}(\gamma^q) = \kappa_\ell^{\Omega/F}(\gamma)^q$ lies in $U_\ell^{(n)}$. So $\gamma^q \in H_{\ell,n}$, and by (i), since $\pi(\gamma)^q = \pi(\gamma^q)$,

$$\pi(\gamma)^q\varphi = \varphi. \tag{3}$$

Let T be the endomorphism $\pi(\gamma) - 1$ of the $\mathbb{Z}_\ell$-module of all functions $C \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$, and let J be the set of polynomials $P \in \mathbb{Z}[Y]$ with $P(T)\varphi = 0$. It is an ideal of the polynomial ring $\mathbb{Z}[Y]$. It contains

$$(Y+1)^q - 1 \qquad \text{and} \qquad \ell^{k_0},$$

the first by (3), since $T + 1 = \pi(\gamma)$, and the second by the choice of k_0. Now q is a power of ℓ, so $(Y+1)^q = Y^q + 1$ in the polynomial ring over the field with ℓ elements. Hence there is $Q \in \mathbb{Z}[Y]$ with

$$(Y+1)^q - Y^q - 1 = \ell\, Q, \qquad \text{that is,} \qquad Y^q = \big((Y+1)^q - 1\big) - \ell\, Q.$$

Modulo J this gives $Y^q \equiv -\ell Q$, and then

$$Y^{qk_0} \equiv (-Q)^{k_0}\, \ell^{k_0} \equiv 0 \pmod{J}.$$

So $T^{qk_0}\varphi = 0$, which is $(\pi(\gamma) - 1)^k\varphi = 0$ for $k = qk_0 = \ell^n k_0$. Finally $\ell^k\varphi = 0$, as $k \geq k_0$. □

The exponent does not depend on γ. For $\ell = 2$ every unit of $\mathbb{Z}_2$ is congruent to 1 modulo 2, so $H_{2,1} = H$ and (ii) holds for every $\gamma \in H$.

5 Where the theorem is used

The archive uses Theorem A in two places outside the unit of this note. Both are stated here as the archive states them. The first is derived from Theorem A(ii) and a proposition that the first note proves; the second uses Theorem A(i) and is not proved here.

Unipotence on the dual. An endomorphism t of a module over $\mathbb{Z}_\ell$ is *unipotent modulo* ℓ if some power of $t - 1$ maps the module into its multiples by ℓ.

Proposition 5.1 (the dual module). *Let ℓ be a prime number, let B be a module over $\mathbb{Z}_\ell$ and f an endomorphism of B. Let t be an endomorphism of the $\mathbb{Z}_\ell$-module $\mathrm{Hom}_{\mathbb{Z}_\ell}(B, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ such that $(t\xi)(\beta) = \xi(f\beta)$ for all $\xi \in \mathrm{Hom}_{\mathbb{Z}_\ell}(B, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ and all $\beta \in B$. Suppose that the module $\mathrm{Hom}_{\mathbb{Z}_\ell}(B, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ is finitely generated over $\mathbb{Z}_\ell$, and that every element of B is killed by a power of $f - 1$. Then t is unipotent modulo ℓ.*

LEAN `PropA.dualUnip`

This is the proposition on the dual module of the first note [N1, §7], where it is proved.

Corollary 5.2 (unipotence on the dual). *Let ℓ be a prime number, F a number field and Ω an algebraic closure of F. Let H be a closed normal subgroup of $\mathrm{Gal}(\Omega/F)$ and $N \geq 0$ an integer such that the module $X_\infty(\ell, N, H)$ is finitely generated over $\mathbb{Z}_\ell$, and write $\pi = \mathscr{F}_{\mathbb{Z}_\ell}(H_{\ell,\infty}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$. Let $\gamma \in H_{\ell,1}$, and let t be the action of γ on $X_\infty(\ell, N, H)$:*

$$(t\xi)(\varphi) = \xi\big(\pi(\gamma^{-1})\varphi\big) \qquad \text{for } \xi \in X_\infty(\ell, N, H),\ \varphi \in D_\infty(\ell, N, H).$$

Then t is unipotent modulo ℓ.

Proof. Put $B = D_\infty(\ell, N, H)$. By Proposition 2.6(a) the operator $\pi(\gamma^{-1})$ maps B to itself; let f be its restriction to B. The element γ^{-1} lies in $H_{\ell,1}$. By Theorem A(ii) for γ^{-1}, the operator $f - 1$ is locally nilpotent on B: every element is killed by a power of it. The module $\mathrm{Hom}_{\mathbb{Z}_\ell}(B, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ is $X_\infty(\ell, N, H)$, which is finitely generated over $\mathbb{Z}_\ell$, and $(t\xi)(\beta) = \xi(f\beta)$. Proposition 5.1 applies. □

LEAN `PropA.xUnip`, by `PropA.dualUnip`

For $H = \mathrm{Gal}(\Omega/F)$ and $N = \ell$ this is how Input 1 of the first note enters the proof of its Theorem D.

Invariants. Part (i) of Theorem A is used in the descent to a layer of the tower [N1, §8, Input 2b], through the following statement.

Proposition 5.3 (invariants). *Let ℓ be a prime number, F a number field and Ω an algebraic closure of F. Let H be a closed normal subgroup of $\mathrm{Gal}(\Omega/F)$, let $N \geq 0$ be an integer and e an integer, and write $\pi = \mathscr{F}_{\mathbb{Z}_\ell}(H_{\ell,\infty}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$. Let V be a subgroup of $\mathrm{Gal}(\Omega/F)$ contained in H, and let $\eta \in V$ be such that every value $\kappa_\ell^{\Omega/F}(g)$, $g \in V$, lies in the closure in $\mathbb{Z}_\ell^\times$ of the set of the powers $\kappa_\ell^{\Omega/F}(\eta)^i$, $i \in \mathbb{Z}$. Then for an element φ of $D_\infty(\ell, N, H)$ the following three conditions are equivalent:*

(1) $\kappa_\ell^{\Omega/F}(g)^{-e}\,\pi(g)\varphi = \varphi$ *for every* $g \in V$;
(2) $\kappa_\ell^{\Omega/F}(\eta)^{-e}\,\pi(\eta)\varphi = \varphi$;
(3) $\kappa_\ell^{\Omega/F}(\eta^{-1})^{-e}\,\pi(\eta^{-1})\varphi = \varphi$.

LEAN `Tower.shaDGen`

The archive states this as two equalities of submodules of $D_\infty(\ell, N, H)$: the elements with (1) are the kernel of the operator $\kappa_\ell^{\Omega/F}(\eta)^{-e}\,\pi(\eta) - 1$, and they are the kernel of the same operator for η^{-1}. For $H = \mathrm{Gal}(\Omega/F)$ it is the statement behind Input 2b of the first note. It belongs to another unit of the archive and is not proved in this note; we only say where Theorem A enters. One needs that an element φ of $D_\infty(\ell, N, H)$ with (2) has (1): that an element fixed by η is fixed by V, for the action twisted by a power of the cyclotomic character. By Theorem A(i) the element is fixed by $H_{\ell,n}$ for some n. This also holds for the twisted action when n is at least the exponent k_0 of Theorem A(ii), because a unit in $U_\ell^{(n)}$ then acts trivially on an element killed by ℓ^{k_0}. And every element of V is the product of a power of η and an element of $H_{\ell,n}$. For $H = \mathrm{Gal}(\Omega/F)$ the group $H_{\ell,n}$ is the group $\mathrm{Gal}(\Omega/F)_{\ell,n}$ of Definition 2.2.

6 Notes on the formal text

1. *The conditions at the places are not used.* The formal statement takes φ in $D_\infty(\ell, N, H)$. Its proof unfolds this hypothesis once and keeps two of its four clauses: φ is locally constant, and it is additive. The clauses on inertia and decomposition groups are not referred to again, and neither is the integer N. So Theorem A holds for every locally constant homomorphism $H_{\ell,\infty} \to \mathbb{Q}_\ell/\mathbb{Z}_\ell$. The conditions matter for Proposition 2.6(a), which makes $D_\infty(\ell, N, H)$ a module with an action of $\mathrm{Gal}(\Omega/F)$.
2. *The exponent.* The formal statement asserts, for each γ, that some k has the two properties of (ii). The proof constructs $k = \ell^n k_0$, the same for all γ; this is the form stated above.

3. *Where the hypotheses on H enter.* Closedness gives the compactness of $H_{\ell,\infty}$, used for the open subgroup W and for the finitely many values, and the compactness of the set K. Normality makes $H_{\ell,\infty}$ normal, so that conjugation acts.
4. *The coefficients.* The module $\mathbb{Q}_\ell/\mathbb{Z}_\ell$ enters through Lemma 3.1(c) alone. The argument of §4 applies to locally constant homomorphisms into any module whose elements are killed by powers of ℓ. This remark is ours; the archive states the theorem for $\mathbb{Q}_\ell/\mathbb{Z}_\ell$.
5. *The polynomial ideal* is the device of the formal proof, followed here step by step. The sketch in the first note used the same congruence, applied k_0 times to elements; the ideal does this bookkeeping once.
6. *The rest of the unit.* The unit of the archive that holds these declarations has 144 declarations that the final theorems use. This note treats 13. The others are, by source file:

The Artin map and class groups	23
Kummer generators, units and Selmer groups	30
Reflection	8
Restriction to the cyclotomic kernel	32
Definitions of the other subjects	38

The grouping is provisional. Each group is the subject of a note to come.

How this note was written. The reading project supplied a dossier of the unit: the statements, a glossary, 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 856 steps of the 103 proofs of the unit, and found that no line of these proofs is left without a step. The proofs of this note were written from those structured proofs. The Lean files of the unit were not opened then; for this edition the definitions were read there, and the proofs were not (see below). The statement of item 1 rests on the quoted lines of the structured proof of the theorem: the hypothesis on φ occurs in four of them and nowhere else. The statements quoted below were read from the archive by the build script, and they agree with the dossier's.

Changes in this edition. The first edition fixed the prime, the number field and its algebraic closure once, at the head of §2, and then wrote the cyclotomic character with one letter, the Galois group with one letter, the groups of the tower with a single index, the module of characters without its ring of coefficients, the two modules at the top of the tower without any argument, and the action by conjugation as a product. That hid arguments of the formal definitions: the fields and the prime in the character and in the groups, the ring in the module of characters, the prime, the integer N and the subgroup in the modules at the top of the tower, and the representation in which an element acts. In this edition every function that the archive defines is written with all the explicit arguments of its formal definition, in every place; the arguments were read from the Lean text of each declaration. The definitions that stood in running text are numbered definitions now, so the items of §2 are renumbered, and every theorem names the prime, the field and its closure in its own statement. Some things are stated that were only described before: the two modules of Definition 2.5, through which Proposition 2.6(c) is phrased as the archive phrases it; and in §5 the two uses of the theorem, with the proposition of the first note that the first of them needs. The second use is quoted without proof. Three letters were renamed, in Definition 2.3 and in the proof of Lemma 3.1, so that none has two meanings. No statement and no proof of the first edition 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 thirteen rows are the declarations of the unit that this note treats.

In this note	Lean declaration	File	Lines
Def. 2.3	`Kum.XDual`	Mk0IdMapCongr.lean	90–99
Def. 2.3	`Kum.Dinf`	Mk0IdMapCongr.lean	195–195
Def. 2.3	`Kum.Xinf`	Mk0IdMapCongr.lean	197–197
Def. 2.4	`Kum.funRep`	Mk0IdMapCongr.lean	121–124
Def. 2.5	`Kum.conjCond`	Mk0IdMapCongr.lean	103–107
Def. 2.5	`Kum.EqHom`	Mk0IdMapCongr.lean	109–110
Def. 2.2	`Kum.Un`	Mk0IdMapCongr.lean	186–186
Prop. 2.6	`Kum.funRepMem`	FunRepMem.lean	5–46
Lemma 3.1(a)	`mem_princ_iff_pow_dvd_sub_one`	DinfNil.lean	7–12
Lemma 3.1(b)	`pow_succ_dvd_pow_prime_sub_one`	DinfNil.lean	14–29
Lemma 3.1(c)	`exists_prime_pow_smul_eq_zero_qz`	DinfNil.lean	31–43
Lemma 3.1(d)	`exists_princ_subset_of_mem_nhds_one`	DinfNil.lean	45–60
Theorem A	`Kum.dinfNil`	DinfNil.lean	62–235
Def. 2.1	`G`	Statement.lean	6–6
Def. 2.1	`QZ`	Statement.lean	15–15
Def. 2.1	`Gal.cycZ`	Global.lean	90–92
Def. 2.3	`Gal.Dec`	Global.lean	15–15
Def. 2.3	`Gal.Ine`	Global.lean	45–64
Def. 2.2	`princ`	LeNuIffPowMemPrinc.lean	16–16
Def. 2.2	`Base.levU`	ConjStableShaFam.lean	187–187
Def. 2.2	`Base.cycU`	ConjStableShaFam.lean	189–189
Def. 2.4	`Base.conjHom`	RestrictionMemInvariantH1.lean	115–118
Prop. 2.6, proof	`conjGal_mem_Dec`	PartsConj.lean	69–75
Prop. 2.6, proof	`conjGal_mem_Ine`	PartsConj.lean	77–81
Cor. 5.2	`PropA.xUnip`	XUnip.lean	9–27
Prop. 5.1	`PropA.dualUnip`	DualUnip.lean	9–34
Prop. 5.3	`Tower.shaDGen`	ShaDGen.lean	9–59

Three statements as they are written in the archive. Theorem A; here `U` is the group H, `levU l U n` is $H_{\ell,n}$, `cycU l U` is $H_{\ell,\infty}$, and `funRep` with its three arguments is the representation π:

```
theorem UpperTheory.V.Kum.dinfNil :
    ∀ (F Ω : Type) [Field F] [NumberField F] [Field Ω] [Algebra F Ω] [IsAlgClosure F Ω] (l : ℕ) [Fact l.Prime] (N
        : ℕ) (U : Subgroup (G F Ω)) [U.Normal], IsClosed (U : Set (G F Ω)) → ∀ φ ∈ Dinf l N U, (∃ n, ∀ g ∈ levU l
        U n, funRep ℤ_[l] (QZ l) (cycU l U) g φ = φ) ∧
    ∀ γ ∈ levU l U 1, ∃ k : ℕ, (l : ℤ_[l]) ^ k • φ = 0 ∧ ((funRep ℤ_[l] (QZ l) (cycU l U) γ - 1) ^ k) φ = 0
```

The module of characters $D_N(C;R,M)$, where `U` is the group C:

```
def XDual (N : ℕ) (U : Subgroup (G F Ω)) (R M : Type) [CommRing R] [AddCommGroup M] [Module R M] : Submodule R (U
    → M) where
  carrier := {φ | IsLocallyConstant φ ∧ (∀ a b, φ (a * b) = φ a + φ b) ∧
    (∀ (A : ValuationSubring Ω) (u : U), u.1 ∈ Ine (F := F) A → φ u = 0) ∧
    ∀ A : ValuationSubring Ω, A.valuation (N : Ω) < 1 → ∀ u : U, u.1 ∈ Dec (F := F) A → φ u = 0}
  zero_mem' := ⟨IsLocallyConstant.const _, by simp, by simp, by simp⟩
  add_mem' {a b} ha hb := ⟨ha.1.add hb.1, fun x y => by simp only [Pi.add_apply, ha.2.1, hb.2.1]; abel,
    fun A u h => by simp [ha.2.2.1 A u h, hb.2.2.1 A u h],
    fun A hA u h => by simp [ha.2.2.2 A hA u h, hb.2.2.2 A hA u h]⟩
  smul_mem' c a ha := ⟨ha.1.comp (c • ·), fun x y => by simp [ha.2.1], fun A u h => by simp [ha.2.2.1 A u h],
    fun A hA u h => by simp [ha.2.2.2 A hA u h]⟩
```

Proposition 2.6:

```
theorem UpperTheory.V.Kum.funRepMem :
    ∀ (F Ω : Type) [Field F] [NumberField F] [Field Ω] [Algebra F Ω] [IsAlgClosure F Ω] (N : ℕ) (U : Subgroup (G
       F Ω)) [U.Normal] (R M : Type) [CommRing R] [AddCommGroup M] [Module R M], (∀ g, ∀ φ ∈ XDual N U R M,
       funRep R M U g φ ∈ XDual N U R M) ∧ (∀ g ∈ U, ∀ φ ∈ XDual N U R M, funRep R M U g φ = φ) ∧
    ∀ (ρ : Representation R (G F Ω) M) (φ : U → M), φ ∈ EqHom N U ρ ↔ φ ∈ XDual N U R M ∧ ∀ g ∈ U, ρ g (funRep R M
       U g φ u) = φ u
```

Notation

The symbols of the text. A name in brackets is the one used in the archive, with the explicit arguments of its definition there.

ℓ, $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$ a prime number; the ring of ℓ-adic integers; its field of fractions

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

F, Ω, E, F_∞ a number field; an algebraic closure of F; a finite extension of F; F with all roots of unity of ℓ-power order

$\mathrm{Gal}(\Omega/F)$ the Galois group of Ω over F [`G F Ω`]

$\kappa_\ell^{\Omega/F}(g)$ the value at g of the ℓ-adic cyclotomic character of Ω over F [`cycZ F Ω l g`]; with a set in the last place, the set of the values on it

ζ a root of unity

$U_\ell^{(n)}$ the units $1+\ell^n\mathbb{Z}_\ell$, with $U_\ell^{(0)}=\mathbb{Z}_\ell^\times$ [`princ l a`]

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

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

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

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

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

$D_N(C;R,M)$ the characters of C with values in M (Definition 2.3) [`XDual N U R M`]

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

$\mathscr{F}_R(C,M)$ the functions $C\to M$ with the action of $\mathrm{Gal}(\Omega/F)$ by conjugation (Definition 2.4) [`funRep R M U`]

π the representation $\mathscr{F}_{\mathbb{Z}_\ell}(H_{\ell,\infty},\mathbb{Q}_\ell/\mathbb{Z}_\ell)$ (Theorem A)

$\mathscr{C}(C;\sigma,\theta)$, $\mathscr{E}_N(C;\rho)$ modules of functions $C\to M$ (Definition 2.5) [`conjCond U σ T`, `EqHom N U ρ`]

σ, θ, ρ an automorphism of the field Ω; an R-linear map $M\to M$; a representation of $\mathrm{Gal}(\Omega/F)$ on M

φ a character, or any function on a subgroup

g, h, γ, η, x, y, c, w, a, b elements of $\mathrm{Gal}(\Omega/F)$

u, v, s, d, r ℓ-adic numbers; $s=1+v+\cdots+v^{\ell-1}$

W, S, K, V an open normal subgroup; the set WC; the set $H\setminus S$; a subgroup of $\mathrm{Gal}(\Omega/F)$ (§5)

n, m, j, i, k, k_0, q, e integers; $\ell^{k_0}\varphi=0$; $q=\ell^n$; e is the exponent of the twist in Proposition 5.3

T, J, P, Q, Y the operator $\pi(\gamma)-1$; the ideal of polynomials that kill φ; polynomials; the indeterminate

B, f, t, ξ, β a module over $\mathbb{Z}_\ell$; an endomorphism of B; an endomorphism of the dual $\mathrm{Hom}_{\mathbb{Z}_\ell}(B,\mathbb{Q}_\ell/\mathbb{Z}_\ell)$; an element of the dual; an element of B

L the number field of 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`.

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