On Euler systems and a conjecture of Coleman

Dominik Bullach David Burns Alexandre Daoud Soogil Seo

We give an explicit, and (up to squaring) complete, classification of Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$ in terms of elementary integer congruences. This result incorporates an inductive construction of infinitely many linearly independent systems that do not belong to the Galois module generated by the cyclotomic system. It also has a range of concrete consequences, including the proof of a long-standing distribution-theoretic conjecture of Robert Coleman and restrictions on the Galois structures of Selmer groups for $\mathbb{G}_m$, and hence of ideal class groups, for real abelian fields.

1 Introduction and statement of main results

The theory of distributions plays a prominent role in number theory research and has been strongly influenced by the classical theory of circular numbers in abelian fields (cf. the discussion of Kubert and Lang in the introduction to [KL81]). In this article, we prove a distribution-theoretic conjecture formulated by Robert Coleman in the late 1980's.

This conjecture (which we henceforth refer to as 'Coleman's Conjecture') predicts an explicit description of the set of so-called 'circular distributions'. The description was originally motivated by an archimedean characterisation of circular units obtained in [Col85] and thereby related to attempts to understand a globalised version of the fact that all norm-compatible families of units in towers of local cyclotomic fields arise by evaluating a Coleman power series at roots of unity, as had earlier been proved in [Col79].

To verify the conjecture, we interpret it in terms of a suitable notion of Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$. To give details, we write Ω° for the set of non-trivial finite abelian extensions of $\mathbb{Q}$. An 'Euler system for $\mathbb{G}_m$ over $\mathbb{Q}$' is then a collection

$$u = (u_E)_E \in \prod_{E \in \Omega^\circ} E^\times$$

that, for every K and L in Ω° with $K \subseteq L$, satisfies the 'distribution relation'

$$\mathrm{N}_{L/K}(u_L) = \big(\prod_\ell (1 - \mathrm{Frob}_\ell^{-1})\big) \cdot u_K. \tag{1}$$

Here $\mathrm{N}_{L/K}$ is the field-theoretic norm map $L^\times \to K^\times$, the product runs over prime numbers ℓ that ramify in L but not K, Frob_ℓ is the arithmetic Frobenius automorphism of ℓ on the maximal abelian extension of $\mathbb{Q}$ in which ℓ is unramified (which acts on $K^\times$ in the obvious way), and we use additive notation for unit groups.

The validity of (1) for every L/K is a strong restriction on a family u. For example, writing $m(K)$ for the finite part of the conductor of a field K in Ω, it implies a containment

$$u_K \in U_K := \begin{cases} \mathcal{O}_K^\times, & \text{if } m(K) \text{ is divisible by two distinct primes,} \\ \mathcal{O}_K[1/m(K)]^\times, & \text{if } m(K) \text{ is a prime-power,} \end{cases} \tag{2}$$

where we write $\mathcal{O}_K$ for the ring of algebraic integers in K (cf. [Seo01, Lem. 2.2]).

Taking account of the Kronecker–Weber Theorem, the 'cyclotomic Euler system' is defined by

$$c := \big(\mathrm{N}_{\mathbb{Q}(m(K))/K}(1 - e^{2\pi i/m(K)})\big)_{K \in \Omega^\circ}, \tag{3}$$

where for any natural number n we set

$$\mathbb{Q}(n) := \mathbb{Q}(e^{2\pi i/n}).$$

2020 *Mathematics Subject Classification.* Primary: 11R04, 11R29; Secondary: 11R23.

Aside from this example, however, the only other Euler systems that have hitherto been identified in this case arise as follows: If Π is any set of odd prime numbers, then the family

$$u_\Pi := (\mathrm{N}_{\mathbb{Q}(m(K))/K}(-1)^{n_{\Pi,K}})_{K\in\Omega^\circ} \tag{4}$$

satisfies (1) for all extensions L/K, where $n_{\Pi,K}$ is defined to be 1 if $m(K)$ is divisible only by primes in Π and to be 0 otherwise.

The collection $\mathcal{E}$ of Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$ is an abelian group under multiplication of systems (so the component of u_1u_2 at K is $u_{1,K}u_{2,K}$ and the identity element is the system $u_\varnothing$ with value 1 on every field in Ω°), and has a natural action of the ring $\mathbb{Z}[\![\Gamma]\!] := \varprojlim_{E\in\Omega^\circ}\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$, where the transition morphisms are the natural restriction maps. We shall derive Coleman's Conjecture from an explicit description of the $\mathbb{Z}[\![\Gamma]\!]$-submodule $\mathcal{E}^{\mathrm{cong}}$ of $\mathcal{E}$ comprising systems u with the property that, for every natural number $n > 1$ and every odd prime number ℓ that does not divide n, one has

$$u_{\mathbb{Q}(\ell n)} \equiv u_{\mathbb{Q}(n)} \quad \text{modulo all } \ell\text{-adic primes of } \mathbb{Q}(\ell n). \tag{5}$$

(These congruences were first used systematically by Thaine in [Tha88] and are well-defined since (2) combines with the fact ℓ is prime to n to imply $u_{\mathbb{Q}(\ell n)}$ and $u_{\mathbb{Q}(n)}$ are both units at all ℓ-adic places.)

To state our description of $\mathcal{E}^{\mathrm{cong}}$ (which will be proved in § 2) we write u_{odd} for the system u_Π defined in (4) with Π the set of all odd primes and $\mathcal{C}$ for the $\mathbb{Z}[\![\Gamma]\!]$-submodule of $\mathcal{E}$ generated by the cyclotomic system c in (3).

(1.1) Theorem. *In $\mathcal{E}$ there is a direct sum decomposition of $\mathbb{Z}[\![\Gamma]\!]$-submodules*

$$\mathcal{E}^{\mathrm{cong}} = \{u_\varnothing, u_{\mathrm{odd}}\} \oplus \mathcal{C}. \tag{6}$$

In particular, Coleman's Conjecture on circular distributions is valid.

We shall give information about Coleman's Conjecture, and how it follows from the equality (6), in § 2.4. For now, we note only that (6) also has a variety of additional consequences, including a distribution-theoretic analogue of the main result of Coleman in [Col85] and the validity of a conjecture of the fourth author in [Seo08] concerning the theory of truncated Euler systems. In addition, (6) also resolves, for each odd p, a deeper, globalised, version of the question of whether the module of Euler systems for the p-adic representation $\mathbb{Z}_p(1)$ over $\mathbb{Q}$ is generated by c over the pro-p completion of $\mathbb{Z}[\![\Gamma]\!]$. The latter possibility is explicitly raised by Mazur and Rubin in [MR04, § 5.3] and so the proof of Theorem (1.1) now leads, via the discussion in loc. cit., to the first example of a representation $T = \mathbb{Z}_p(1)$ for which [MR04, Question 5.3.21] has been answered (this question concerns Kolyvagin-derivative homomorphisms and is described in loc. cit. as being 'very difficult').

There are several obstacles to overcome to prove Theorem (1.1). Firstly, the result concerns systems defined integrally (that is, over $\mathbb{Z}$) rather than either p-adically for a fixed prime p or adelically and so, since $\mathbb{Z}[\![\Gamma]\!]$ is neither noetherian nor compact, many standard algebraic techniques do not apply. In addition, for any prime p, the splitting of p-adic places forces many of the relations (1) to be trivial, and so limits the effectiveness of techniques of classical (p-adic) Iwasawa theory in this setting. Indeed, issues of this kind have hitherto only ever been resolved in cases where the Euler system is both given explicitly and directly related to L-values, and in each such case the resolution relies on deep results such as a derivative formula for an associated p-adic L-series or a description of the constant term of an associated Coleman power series. For these reasons, a resolution of Coleman's Conjecture has until now seemed out of reach, with comparatively little supporting evidence and no proof strategy apparent (see [Seo01] or [BS21] for a discussion of the history).

To address these issues, we systematically incorporate arguments from (what one might call) 'horizontal' Iwasawa theory. That is, rather than focusing for each p on p-cyclotomic towers, we also study the values of Euler systems over a large, carefully chosen, family of extensions

that are unramified at p. In fact, we find that such a blending of techniques of classical and horizontal Iwasawa theory has consequences far beyond Coleman's Conjecture, including to the study of special value conjectures. For example, it gives rise to a novel, and effective, strategy to obtain evidence for, and in some important cases prove, a strictly refined version of the (equivariant) Tamagawa Number Conjecture for $\mathbb{G}_m$ over general number fields (though, for brevity, these results are deferred to the article [Bul+23]). In addition, it has surprising consequences for the study of general Euler systems, and Selmer groups, for $\mathbb{G}_m$ over $\mathbb{Q}$.
To discuss the latter results we note the relations (1) imply that for any Euler system u and prime p the elements u_L form a norm compatible family as L ranges over fields for which $m(L)$ is a power of p, and hence that the valuation $\mathrm{Ord}_p(u)$ of u_L at the unique p-adic place of L is independent of L. In this way, writing $\mathscr{P}$ for the set of all prime numbers, one obtains a homomorphism of $\mathbb{Z}[\![\Gamma]\!]$-modules

$$\mathrm{Ord}_{\mathbb{Q}}\colon \mathcal{E} \to \prod_{\ell\in\mathscr{P}} \mathbb{Z}, \quad u \mapsto (\mathrm{Ord}_\ell(u))_\ell.$$

We write ϖ for the diagonal map $\mathbb{Z} \to \prod_{\ell\in\mathscr{P}} \mathbb{Z}$ and use congruences to define an explicit subgroup of $\prod_{\ell\in\mathscr{P}} \mathbb{Z}$ that contains $\varpi(\mathbb{Z})$ by setting

$$\Theta := \Big\{ (m_\ell)_\ell \in \prod_{\ell\in\mathscr{P}} \mathbb{Z} \mid m_p \equiv m_q \text{ modulo } p^{\mathrm{ord}_p((q-1)/2)} \text{ for all primes } p < q \Big\}. \tag{7}$$

We also write $\mathcal{T}$ for the $\mathbb{Z}[\![\Gamma]\!]$-submodule of $\mathcal{E}$ generated by all systems u_Π as in (4), and $\mathcal{C}^0$ for the $\mathbb{Z}[\![\Gamma]\!]$-submodule of $\mathcal{C}$ comprising systems of the form $r(c)$ with r an element of the kernel of the projection map $\mathbb{Z}[\![\Gamma]\!] \to \mathbb{Z}$. We can now state our main result concerning the map $\mathrm{Ord}_{\mathbb{Q}}$.

(1.2) Theorem. *One has* $2\cdot\Theta \subseteq \mathrm{im}(\mathrm{Ord}_{\mathbb{Q}}) \subseteq \Theta$*,* $\ker(\mathrm{Ord}_{\mathbb{Q}}) = \mathcal{T} + \mathcal{C}^0$ *and*

$$\{u \in \mathcal{E} \mid \mathrm{Ord}_{\mathbb{Q}}(u) \in \varpi(\mathbb{Z})\} = \mathcal{T} + \mathcal{C}.$$

Our proof of this result is given in § 3 and incorporates an inductive construction of a pre-image under $\mathrm{Ord}_{\mathbb{Q}}$ of every element of $2\cdot\Theta$ and so gives an explicit description, up to squaring, of the full module of Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$ (and see also Remark (3.7) (ii) for a cleaner statement in this direction). This is, it seems, the first complete classification of Euler systems in any natural setting and has some interesting consequences. For instance, the result directly implies that any u in $\mathcal{E}$ for which $\mathrm{Ord}_p(u)$ is independent of p belongs to $\mathcal{T} + \mathcal{C}$, and also that the quotient $\mathcal{E}/(\mathcal{T} + \mathcal{C})$ is torsion-free and cannot be generated over $\mathbb{Z}[\![\Gamma]\!]$ by finitely many elements (see Theorem (3.1) (iii)). This shows that, despite the previously apparent scarcity of Euler systems, cyclotomic systems in fact account for a remarkably small proportion of all Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$.
We recall next that the 'integral dual Selmer group' $\mathcal{S}(\mathbb{G}_{m/K})$ of $\mathbb{G}_m$ over a number field K is a classically defined object that is related to the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ of K by means of a canonical short exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cl}(\mathcal{O}_K), \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathcal{S}(\mathbb{G}_{m/K}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_K^\times, \mathbb{Z}) \longrightarrow 0 \tag{8}$$

(for more details see § 4). We are now able to deduce from Theorem (1.2) the following result about the Galois structure of these modules as K varies over real fields in Ω. In this result we refer to a subset $\mathcal{X}$ of Ω_+ as 'dense' if, for every K in Ω_+°, there exists a field E in $\mathcal{X}$ such that $K \subseteq E$ and $m(E)$ and $m(K)$ have the same prime divisors. In addition, for K in Ω_+ and an ideal I of $\mathbb{Z}[\Gamma_K]$ we write I^{-1} for the 'inverse' $\{x \in \mathbb{Q}[\Gamma_K] \mid x \cdot I \subseteq \mathbb{Z}[\Gamma_K]\}$.

(1.3) Theorem. *For any dense subset* $\mathcal{X}$ *of* Ω_+ *one has*

$$\Big(\prod_{K\in\mathcal{X}} \mathrm{Fitt}^1_{\mathbb{Z}[\Gamma_K]}(\mathcal{S}(\mathbb{G}_{m/K}))\Big) \cap \mathbb{Q}[\![\Gamma^+]\!] = 0 \quad \textit{and} \quad \Big(\prod_{K\in\mathcal{X}} \mathrm{Fitt}^1_{\mathbb{Z}[\Gamma_K]}(\mathcal{S}(\mathbb{G}_{m/K}))^{-1}\Big) \cap \mathbb{Q}[\![\Gamma^+]\!] = \mathbb{Z}[\![\Gamma^+]\!].$$

Whilst the proof of the first equality here relies on Kummer theory and class field theory, the proof of the second lies deeper and depends crucially on Theorem (1.2). In addition, these equalities control the Galois structure of Selmer groups and hence, via (8), of class groups and unit groups in a fashion that is both non-trivial and independent of L-series (see § 4.3). In particular, this last observation implies such restrictions are not implicit in the formalism of leading term conjectures such as the (equivariant) Tamagawa number conjecture.

To end the introduction, we shall now for the reader's convenience collect together some general notation that will be used throughout the article.

We write $\mathbb{Q}^{\mathrm{ab}}$ for the maximal abelian extension of $\mathbb{Q}$ in $\mathbb{C}$, and then set $\mathbb{Q}^{\mathrm{ab},+} := \mathbb{Q}^{\mathrm{ab}} \cap \mathbb{R}$, $\Gamma := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and $\Gamma^+ := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab},+}/\mathbb{Q})$. We write Ω and Ω_+ for the set of finite extensions of $\mathbb{Q}$ in $\mathbb{Q}^{\mathrm{ab}}$ and $\mathbb{Q}^{\mathrm{ab},+}$, and set $\Omega^\circ := \Omega \setminus \{\mathbb{Q}\}$ and $\Omega^\circ_+ := \Omega^+ \setminus \{\mathbb{Q}\}$. For K in Ω we set $\Gamma_K := \mathrm{Gal}(K/\mathbb{Q})$ and, for a commutative ring Λ, we consider the inverse limit rings

$$\Lambda[\![\Gamma]\!] := \varprojlim_{K \in \Omega} \Lambda[\Gamma_K] \quad \text{and} \quad \Lambda[\![\Gamma^+]\!] := \varprojlim_{K \in \Omega_+} \Lambda[\Gamma_K], \tag{9}$$

where the transition morphisms are the natural restriction maps $\pi_{L/K,\Lambda}\colon \Lambda[\Gamma_L] \to \Lambda[\Gamma_K]$ for $K \subseteq L$. (In the sequel we abbreviate $\pi_{L/K,\mathbb{Z}}$ to $\pi_{L/K}$).

For $u \in \mathcal{E}$ and $r = (r_K)_K \in \mathbb{Z}[\![\Gamma]\!]$ we write either $r \cdot u$ or $r(u)$ for the family $(r_K(u_K))_K \in \mathcal{E}$.

Acknowledgements We are very grateful to Takenori Kataoka for spotting an error in an earlier argument related to results presented here and also to Andreas Nickel for several helpful comments and discussions. We also note that parts of this article incorporate results from the first author's PhD thesis.

The first and second authors would like to thank the Mathematics Department of Yonsei University, Seoul, for its generous hospitality at a key point in this project. The first and third authors wish to acknowledge the financial support of the Engineering and Physical Sciences Research Council [EP/L015234/1, EP/N509498/1, EP/W522429/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory ('The London School of Geometry and Number Theory'), University College London and King's College London.

2 Congruence Euler systems and the proof of Theorem (1.1)

2.1 p-adic considerations

In this section we fix a prime p and prove some key results about certain auxiliary modules of p-adically valued Euler systems. To do this, we set

$$p^* := \begin{cases} p, & \text{if } p \text{ is odd} \\ 4, & \text{if } p = 2, \end{cases}$$

and write $\Omega(p)$ for the subset of Ω comprising fields K with the property that $m(K)$ is divisible by p. We then consider the following notions of Euler system.

(2.1) Definition.

(i) For a commutative algebra A the group $\mathcal{E}_A$ of 'A-valued Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$' is the subset of $\prod_{E \in \Omega^\circ}(A \otimes_{\mathbb{Z}} U_E)$ comprising elements that satisfy the distribution relation (1) for all L and K. In the case $A = \mathbb{Z}_p$ for a prime p, we abbreviate $\mathcal{E}_A$ to $\mathcal{E}_p$ and refer to it as the group of 'p-adic Euler systems for $\mathbb{G}_m$ over $\mathbb{Q}$'.

(ii) The group $\mathcal{E}(p)$ of 'Euler systems for $\mathbb{Z}_p(1)$ over $\mathbb{Q}$' is the set comprising elements of $\prod_{E \in \Omega(p)}(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_E[1/p]^\times)$ that satisfy (1) for all L and K.

The groups $\mathcal{E}_p$ and $\mathcal{E}(p)$ are both modules over $\mathbb{Z}_p[\![\Gamma]\!]$. In addition, $\mathcal{E}(p)$ fits into the framework of Euler systems for p-adic representations as defined by Rubin in [Rub00, Def. 2.1.1]. These groups are also related by a composite 'restriction' morphism of $\mathbb{Z}[\![\Gamma]\!]$-modules

$$\iota_p : \mathcal{E} \to \mathcal{E}_p \to \mathcal{E}(p), \quad (c_K)_{K\in\Omega^o} \mapsto (1\otimes c_K)_{K\in\Omega} \mapsto (1\otimes c_K)_{K\in\Omega(p)},$$

where $1\otimes c_K$ is the image of c_K under the natural map $U_K \to \mathbb{Z}_p\otimes_{\mathbb{Z}} U_K$. In the sequel we also use 'ι_p' to denote the homomorphism of $\mathbb{Z}_p[\![\Gamma]\!]$-modules $\mathcal{E}_p \to \mathcal{E}(p)$ given by the second map in this composite (with the precise meaning always being clear from context).
We write τ for the element of Γ induced by complex conjugation, and set $T_\tau := 1+\tau \in \mathbb{Z}[\![\Gamma]\!]$.

(2.2) Proposition. *The $\mathbb{Z}_p[\![\Gamma]\!]$-module $T_\tau(\mathcal{E}(p))$ is cyclic, with generator $\iota_p(T_\tau(c))$.*

Proof. Setting $R_p := \mathbb{Z}_p[\![\Gamma]\!]$, it is clear that $R_p\cdot\iota_p(c) \subseteq \mathcal{E}(p)$. It is therefore enough to fix v in $\mathcal{E}(p)$ and show that $T_\tau(v)$ is an R_p-multiple of $\iota_p(T_\tau(c))$. To do this, we will rely on two results from [BS21]. Firstly, for any such v the argument of [BS21, Th. 3.1] implies that $v_L \in R_p\cdot c_L$ for all L in $\Omega(p)$. This containment implies that the family $T_\tau(v)$ belongs to the R_p-module $\mathcal{V}_p^d$ defined in [BS21, § 5.3.1] and so it is enough to recall [BS21, Prop. 5.3 (i)] asserts that $\mathcal{V}_p^d$ is a free R_p-module of rank one, with generator $\iota_p(T_\tau(c))$. □

For K in Ω and x in U_K we write x_p for the image of x in $\mathbb{Z}_p\otimes_{\mathbb{Z}} U_K$.

(2.3) Proposition. *The following claims are valid.*

(i) If $v=(v_K)_K \in T_\tau(\mathcal{E}_p)$ belongs to $\ker(\iota_p)$, then for all $K\in\Omega^\circ$ the element v_K belongs to the submodule $\mathbb{Z}_p\otimes_{\mathbb{Z}}(U_K)^{\Gamma_K}$ of $\mathbb{Z}_p\otimes_{\mathbb{Z}} U_K$.

(ii) If $v=(v_K)_K\in T_\tau(\mathcal{E})$ satisfies the congruences (5), then there exists an element r_p of $\mathbb{Z}_p[\![\Gamma]\!]$ such that, for every $K\in\Omega^\circ$, one has $T_\tau(v_K)_p = r_p\cdot T_\tau(c_K)_p$ in $\mathbb{Z}_p\otimes_{\mathbb{Z}} T_\tau(U_K)$.

Proof. Fix v in $\mathcal{E}_p$ that belongs to $\ker(\iota_p)$. Then v_K is trivial for every K in $\Omega(p)$ and, in particular, belongs to $(\mathbb{Z}_p\otimes_{\mathbb{Z}} U_K)^{\Gamma_K} = \mathbb{Z}_p\otimes_{\mathbb{Z}}(U_K)^{\Gamma_K}$ for such K. To prove claim (i) it is therefore enough to fix a field K in $\Omega\setminus\Omega(p)$ and show v_K is fixed by the action of Γ_K.
To do this we fix a natural number $n>1$ and define an auxiliary field by setting

$$k(p,n) := \begin{cases} \mathbb{Q}(p^n) & \text{if } p \text{ is odd,}\\ \mathbb{Q}(2^{n+1})(\sqrt[4]{2}) & \text{if } p=2.\end{cases}$$

This field is disjoint from K. Indeed, if not, then $K\cap k(p,n)$ would be a ramified extension of $\mathbb{Q}$ and this is impossible since K is unramified at p whilst $k(p,n)$ is unramified outside p.
In particular, since K and $k(p,n)$ are disjoint, the theory of embedding problems implies (via, for example, [Bul+23, Prop. 4.14]) that, for each σ in Γ_K, there exists a real cyclic p-extension $E=E(p,n,\sigma)$ of $\mathbb{Q}$ with the following three properties:

(P_1) p is unramified in E and the order of Frob_p on E is at least p^n,

(P_2) at most two prime numbers ramify in E, and each of these is unramified in K,

(P_3) if ℓ is a prime number that ramifies in E, then the restriction of Frob_ℓ to K is equal to σ.

To proceed, we set $L := \mathbb{Q}(p\cdot m(K))$ and $F := E\cdot L$. Note that L and F both belong to $\Omega(p)$, and hence that v_L and v_F both vanish. By (P_1) we know that E, and hence also EK, is unramified at p and so (1) implies that

$$0 = \mathrm{N}_{F/EK}(0) = \mathrm{N}_{F/EK}(v_F) = (1-\mathrm{Frob}_p^{-1})(v_{EK}).$$

This shows that v_{EK} is fixed by Frob_p, and hence also by every element in the subgroup H of $\mathrm{Gal}(EK/K)$ generated by $\mathrm{Frob}_p^{[K:\mathbb{Q}]}$. Note that $|H|\geq p^{n-\mathrm{ord}_p([K:\mathbb{Q}])}$ as a consequence of (P_2).
The relation (1) now combines with (P_2) and (P_3) to yield that there is $i\in\{1,2\}$ such that

$$(1-\sigma)^i(v_K) = \mathrm{N}_{EK/K}(v_{EK}) = \mathrm{N}_{EK^H/K}(\mathrm{N}_{EK/EK^H}(v_{EK})) = |H|\cdot\mathrm{N}_{EK^H/K}(v_{EK})$$

is divisible by $|H|$ in the finitely generated $\mathbb{Z}_p$-module U_K. Since $\mathrm{ord}_p(|H|)$ is unbounded as n increases, it follows that $(1-\sigma)^2(v_K)$ vanishes.

Write $e_{\mathbf{1}}$ for the idempotent $|\langle\sigma\rangle|^{-1}\sum_{h\in\langle\sigma\rangle} h$ of $\mathbb{Q}[\langle\sigma\rangle]$ and note $1-e_{\mathbf{1}}$ belongs to the augmentation ideal of $\mathbb{Q}[\langle\sigma\rangle]$. Since the latter ideal is generated by $1-\sigma$, it follows that $1-e_{\mathbf{1}} = x(1-\sigma)$ for some $x \in \mathbb{Q}[\langle\sigma\rangle]$, and hence also

$$x(1-\sigma)^2 = (1-\sigma)\big(x(1-\sigma)\big) = (1-\sigma)(1-e_{\mathbf{1}}) = (1-\sigma).$$

Thus, if we now fix a natural number z such that $z\cdot x \in \mathbb{Z}[\langle\sigma\rangle]$, then this computation combines with the previous discussion to imply that the element

$$z\cdot(1-\sigma)(v_K) = z\cdot x\cdot(1-\sigma)^2(v_K)$$

is divisible by $|H|$. Taking n to be large, we deduce $z(1-\sigma)(v_K)$ vanishes and hence that $(1-\sigma)(v_K)$ vanishes since v_K belongs to the $\mathbb{Z}$-torsion free group $T_\tau(U_K)$. This shows that v_K is fixed by every element of Γ_K, as required to prove claim (i).

To prove claim (ii), we fix an Euler system v in $\ker(\iota_p)$ that satisfies the congruences (5). Then, by Proposition (2.2) there exists $r_p = (r_{p,K})_K$ in R_p such that $\iota_p(T_\tau(v)) - r_p(\iota_p(T_\tau(c)))$ is trivial, and hence $v' := T_\tau(v - r_p(c)) \in \ker(\iota_p)$. It follows from claim (i) that $v'_K := T_\tau(v_K - r_{p,K}(c_K))$ belongs to $\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathbb{Q}^\times$ for every $K\in\Omega$. We now claim that this implies v'_K vanishes if $m(K)$ is composite. To prove this, it suffices to show $v'_{\mathbb{Q}(m(K))}$ vanishes if $m(K)=\ell^t n$ with ℓ prime, $t\in\mathbb{N}$ and $n\in\mathbb{N}\setminus\{1\}$ prime to ℓ. Then, since $v'_{\mathbb{Q}(m(K))}$ is Γ-invariant and belongs to the $\mathbb{Z}$-torsion free group $\mathbb{Z}_p\otimes_{\mathbb{Z}} T_\tau(U_{\mathbb{Q}(m(K))})$ one has

$$[\mathbb{Q}(m(K)):\mathbb{Q}]\cdot v'_{\mathbb{Q}(m(K))} = \mathrm{N}_{\mathbb{Q}(m(K))/\mathbb{Q}}(v'_{\mathbb{Q}(m(K))}) = \mathrm{N}_{\mathbb{Q}(m(K))/\mathbb{Q}(n)}\big((1-\mathrm{Frob}_\ell^{-1})\cdot v'_{\mathbb{Q}(n)}\big) = 0,$$

and so $v'_{\mathbb{Q}(m(K))}$ vanishes.

Write the element $r_{p,K}$ as a family $(r_{p,K,n})_{n\in\mathbb{N}}$ in $\mathbb{Z}_p[\Gamma_K] = \varprojlim_{n\in\mathbb{N}}((\mathbb{Z}/p^n\mathbb{Z})[\Gamma_K])$. Then, since v'_K vanishes, for every n the element $T_\tau(v_K - r_{p,K,n}(c_K))$ is divisible by p^n in the (torsion-free) group $T_\tau(U_K)$. This in turn implies that the family $v'_n := T_\tau(v_K - r_{p,K,n}(c_K))_{K\in\Omega^\circ}$ is an Euler system that satisfies (5) and is such that $2v'_{n,K}$ is a $2p^n$-th power in U_K whenever $m(K)$ is composite.

We claim this implies $2v'_{n,K}$ is a p^n-th power in U_K for *every* K in Ω°. To prove this, it suffices to show $2v'_{n,\mathbb{Q}(q)}$ is a p^n-th power for every prime power q. By [NSW08, Th. 9.1.1 (ii)], it is then enough to show $2v_{n,\mathbb{Q}(q)}$ is a $2p^n$-th power in the completion of $\mathbb{Q}(q)$ at every non-archimedean place $\wp$ that is prime to $2pq$. We fix such a place $\wp$ of $\mathbb{Q}(q)$ and write $\mathbb{F}_\wp$ for the residue field of $\mathcal{O}_{\mathbb{Q}(q)}$ at $\wp$. Then, since $v'_{n,\mathbb{Q}(q)}$ is a q-unit (and so integral at $\wp$) and $\wp$ is prime to $2p$, Hensel's Lemma reduces us to showing $2v'_{n,\mathbb{Q}(q)}$ is a $2p^n$-th power in $\mathbb{F}_\wp^\times$. To do this we write ℓ for the characteristic of $\wp$ and fix a place $\wp'$ of $\mathbb{Q}(\ell q)$ above $\wp$. Then $2v'_{n,\mathbb{Q}(\ell q)}$ is a $2p^n$-th power in $\mathbb{Q}(\ell q)$ and so the congruence (5) implies $2v'_{n,\mathbb{Q}(q)}$ is a $2p^n$-th power in the residue field $\mathbb{F}_{\wp'}$ of $\mathcal{O}_{\mathbb{Q}(\ell q)}$ at $\wp'$. In addition, since $\wp$ is totally ramified in the extension $\mathbb{Q}(\ell q)/\mathbb{Q}(q)$, the inclusion map $\mathbb{F}_\wp \to \mathbb{F}_{\wp'}$ is an isomorphism of fields and so $2c'_{n,\mathbb{Q}(q)}$ is a $2p^n$-th power in $\mathbb{F}_\wp$, as we wished to show. We have therefore proved that $2v'_K = (2v'_{n,K})_{n\in\mathbb{N}}$ vanishes in $\mathbb{Z}_p\otimes_{\mathbb{Z}} U_K$. Hence, as v'_K belongs to the $\mathbb{Z}$-torsion-free subgroup $\mathbb{Z}_p\otimes_{\mathbb{Z}} T_\tau(U_K)$, we can conclude $v'_K = 0$.

From the equality $v'_K = 0$ we can therefore conclude that $T_\tau(v_K)_p = r_p\cdot T_\tau(c_K)_p$ for every K in Ω°, as required to complete the proof of claim (ii). □

2.2 Annihilators of cyclotomic units

In this section we prove some useful technical results concerning the Galois structure of modules generated by Euler systems.

We write Δ^* for the character group $\mathrm{Hom}(\Delta,\mathbb{C}^\times)$ of a finite abelian group Δ. For each $\chi\in\Delta^*$ we write e_χ for the idempotent $|\Delta|^{-1}\sum_{\delta\in\Delta}\chi(\delta^{-1})\delta$ of $\mathbb{Q}^{\mathrm{ab}}[\Delta]$ and, if χ is the trivial homomorphism, we often write e_Δ in place of e_χ.

For K in Ω we set $K^+ := \mathbb{R}\cap K$ and $\Gamma_K^+ := \Gamma_{K^+}$, and define an ideal of $\mathbb{Z}[\Gamma_K^+]$ by setting

$$I_K := \{r\in\mathbb{Z}[\Gamma_K^+] \mid r(T_\tau(c_K)) = 0\}.$$

In the next result we describe explicitly this annihilator ideal in terms of the idempotent of $\mathbb{Q}[\Gamma_K^+]$ that is obtained by setting

$$e_K := \begin{cases} 1, & \text{if } m(K) \text{ is a prime power,} \\ \prod_{\ell \mid m(K)}(1 - e_{D_{K,\ell}}), & \text{otherwise,} \end{cases} \tag{10}$$

where ℓ runs over prime divisors of $m(K)$ and $D_{K,\ell}$ is the decomposition subgroup of ℓ in Γ_K^+.

(2.4) Proposition. *For every field K in Ω the following claims are valid.*

(i) I_K is equal to the set $\{x \in \mathbb{Z}[\Gamma_K^+] \mid e_K \cdot x = 0\}$.

(ii) If $\psi \in \Gamma_K^{+,*}$ is such that $e_\psi e_K = 0$, then $m(K)$ is not a prime power and ψ is trivial on the decomposition group in Γ_K^+ of a prime divisor of $m(K)$.

(iii) If u belongs to $T_\tau(\mathcal{E})$, then the image of u_K in $\mathbb{Q} \otimes_\mathbb{Z} U_K$ belongs to $\mathbb{Q}[\Gamma_K^+] \cdot T_\tau(c_K)$.

Proof. Claim (i) is proved in [BS21, Lem. 2.4] and relies on the link between cyclotomic elements and first derivatives of Dirichlet L-series (as discussed, for example, in [Tat84, Ch. 3, § 5]). Claim (ii) follows directly from the explicit description (10) of e_K and the fact that for each subgroup H of Γ_K^+ one has $e_\psi(1 - e_H) = 0$ if ψ is trivial on H and $e_\psi(1 - e_H) = e_\psi$ otherwise. To prove claim (iii) we use the fact that the natural map $\iota\colon K^\times \to \mathbb{Q}^{\mathrm{ab}} \otimes_\mathbb{Z} K^\times$ is injective on the torsion-free subgroup $T_\tau(K^\times)$ of $K^\times$. We write $u = T_\tau(w)$ with $w \in \mathcal{E}$ and claim first that the image of $u_K = T_\tau(w_K)$ under ι is stable under multiplication by e_K. In view of claim (ii), to show this it is enough to prove for every ψ in $\Gamma_K^{+,*}$ that if $e_\psi \cdot \iota(u_K) \neq 0$, then ψ cannot be trivial on the decomposition group of any prime that ramifies in K (and so $e_\psi e_K = e_\psi$).
To see this, we write π for the restriction map $\Gamma_K \to \Gamma_K^+$ and note, for each ψ in $\Gamma_K^{+,*}$, that

$$\begin{aligned} e_\psi \cdot \iota(u_K) &= e_{\psi\circ\pi} \cdot T_\tau \iota(w_K) \\ &= 2 \cdot e_{\psi\circ\pi} \cdot \iota(w_K) \\ &= 2 \cdot \Big(\prod_{\ell \in \mathscr{P}_\psi} (1 - \psi(\mathrm{Frob}_\ell^{-1})) \Big) \cdot e_{\psi\circ\pi} \cdot \iota(w_{K_\psi}) \\ &= \Big(\prod_{\ell \in \mathscr{P}_\psi} (1 - \psi(\mathrm{Frob}_\ell^{-1})) \Big) \cdot e_\psi \cdot \iota(u_{K_\psi}). \end{aligned}$$

Here K_ψ denotes the subfield of K fixed by $\ker(\psi \circ \pi)$ (or equivalently, the subfield of K^+ fixed by $\ker(\psi)$) and $\mathscr{P}_\psi$ is the set of primes that ramify in K but not in K_ψ. In addition, the first of the equalities is clear, the second and fourth are true since the image of τ in Γ_K is contained in $\ker(\psi \circ \pi)$, and the third equality is true since the system w validates (1).
From the above equalities it is clear that, if $e_\psi \cdot \iota(u_K) \neq 0$, then $\ker(\psi)$ cannot contain Frob_ℓ for any ℓ in $\mathscr{P}_\psi$. On the other hand, any prime ℓ that ramifies in K but does not belong to $\mathscr{P}_\psi$ is ramified in K_ψ and so its inertia group in Γ_K^+ is not contained in $\ker(\psi)$. Hence, if $e_\psi \cdot \iota(u_K) \neq 0$, then ψ cannot be trivial on the decomposition group in Γ_K^+ of any prime that ramifies in K, as required.
Now, since $w_K \in U_K$ (by (2)), the above argument implies $\iota(u_K) \in e_K(\mathbb{Q} \otimes_\mathbb{Z} T_\tau(U_K))$. To prove claim (iii) it is thus enough to show that the $\mathbb{Q}[\mathcal{G}_K^+]$-module $e_K(\mathbb{Q} \otimes_\mathbb{Z} T_\tau(U_K))$ is generated by $T_\tau(c_K)$. But this is true since if $\psi \in \Gamma_K^{+,*}$ is such that $e_\psi e_K \neq 0$, then claim (i) combines with the fact $c_K \in U_K$ to imply $e_\psi(\iota(T_\tau(c_K))) \in e_\psi(\mathbb{Q}^{\mathrm{ab}} \otimes_\mathbb{Z} (T_\tau(U_K)) \setminus \{0\}$, whilst one also has

$$\dim_{\mathbb{Q}^{\mathrm{ab}}}\big(e_\psi(\mathbb{Q}^{\mathrm{ab}} \otimes_\mathbb{Z} T_\tau(U_K))\big) = \dim_{\mathbb{Q}^{\mathrm{ab}}}\big(e_{\psi\circ\pi}(\mathbb{Q}^{\mathrm{ab}} \otimes_\mathbb{Z} X_K)\big) = 1.$$

Here we write X_K for the subgroup of the free abelian group on the set of archimedean places of K if $m(K)$ is divisible by two distinct primes, respectively the set of places of K that are either archimedean or p-adic if $m(K)$ is a power of p, comprising elements whose coefficients sum to zero. The first equality is therefore true since the Dirichlet Regulator map induces an isomorphism of $\mathbb{C}[\Gamma_K]$-modules $\mathbb{C} \otimes_\mathbb{Z} U_K \cong \mathbb{C} \otimes_\mathbb{Z} X_K$ (cf. [Tat84, Ch. I, § 4.2]) and the second follows by a straightforward computation from the definition of X_K. □

2.3 The characterisation of $\mathcal{E}^{\mathrm{cong}}$

In this section we prove the explicit description of $\mathcal{E}^{\mathrm{cong}}$ claimed in (6).

At the outset we recall that, as proved by the third author in [Seo06, Th. 2.5], the abelian group $\mathcal{C}$ is torsion-free and thereby disjoint from $\mathcal{T}$. It is also straightforward to check explicitly that $u_\varnothing$ and u_{odd} are the only systems in $\mathcal{T}$ that satisfy the congruences (5). To prove (6) it is therefore enough to show that $\mathcal{E}^{\mathrm{cong}}$ is contained in $\mathcal{T}+\mathcal{C}$ and our proof of this fact will occupy the remainder of this section.

We first make several useful deductions from results of [BS21]. To do this we set

$$R \coloneqq \mathbb{Z}[\![\Gamma]\!],\ \ R^+ \coloneqq \mathbb{Z}[\![\Gamma^+]\!] \quad \text{and} \quad \widehat{R^+} \coloneqq \varprojlim_{K\in\Omega} \widehat{\mathbb{Z}}[\Gamma_{K^+}],$$

where $\widehat{\mathbb{Z}}$ denotes the profinite completion of $\mathbb{Z}$. We also fix u in $\mathcal{E}^{\mathrm{cong}}$ and define R^+-modules

$$\mathcal{C}^+ \coloneqq T_\tau(\mathcal{C}),\ Y = Y_u \coloneqq R^+\cdot T_\tau(u) \ \text{ and } \ X = X_u \coloneqq (\mathcal{C}^+ + Y)/\mathcal{C}^+.$$

Then, in view of the observations made above, the following result reduces the proof of (6) to showing that (for every u) the module X vanishes.

(2.5) Lemma. *For every v in $\mathcal{E}$, there exists an exact sequence of R-modules*

$$0 \to \mathcal{T}+\mathcal{C} \overset{\subseteq}{\to} \mathcal{T}+\mathcal{C}+R\cdot v \xrightarrow{z\mapsto T_\tau(z)} X_v \to 0 \tag{11}$$

Proof. Since $T_\tau(y)=0$ for every $y\in\mathcal{T}$ one has $T_\tau(z)\in\mathcal{C}^+ + Y$ for each $z\in\mathcal{T}+\mathcal{C}+R\cdot v$ and so the assignment $z\mapsto T_\tau(z)$ induces a well-defined surjective homomorphism of R-modules t from $\mathcal{T}+\mathcal{C}+R\cdot v$ to X.

Now, with this definition of t, it is clear $\mathcal{T}+\mathcal{C}$ is contained in $\ker(t)$ and hence enough to show that if $t(z)=0$, then z belongs to $\mathcal{T}+\mathcal{C}$. Moreover, if $t(z)=0$, then there exists an element r of R such that $T_\tau(z)=r\cdot T_\tau(c)$. It follows that $T_\tau\cdot(z-r(c))=0$ and hence, by [BS21, Th. 4.1 (i)], that $z-r(c)$ belongs to $\mathcal{E}_{\mathrm{tor}}+R(1-\tau)(c)$. Since this implies that z belongs to $\mathcal{E}_{\mathrm{tor}}+\mathcal{C}$, it is therefore enough to recall that $\mathcal{E}_{\mathrm{tor}}=\mathcal{T}$ (by [Seo04, Th. B]). □

To show that $X=X_u$ vanishes we note that the restriction map

$$\pi\colon R\to R^+, \quad (r_K)_K \mapsto (\pi_K(r_K))_{K^+}$$

is surjective, where we set $\pi_K \coloneqq \pi_{K/K^+}$. This is true since each π_K is surjective with kernel $(1-\tau)\mathbb{Z}[\Gamma_K]$ and the derived limit $\varprojlim^1_{K\in\Omega}((1-\tau)\mathbb{Z}[\Gamma_K])$ with respect to the transition maps induced by $\pi_{L/K}$ for $K\subset L$ vanishes as a consequence of the Mittag–Leffler condition.

It follows that $\mathcal{C}^+ = R^+\cdot T_\tau(c)$ and so it suffices, by Lemma (2.5), to show the existence of an element $r=r_u$ of R^+ such that $T_\tau(u)=r(T_\tau(c))$.

We note first that, as a consequence of Proposition (2.3) (ii), for every prime number p there exists an element $r_p=r_{p,u}$ of R^+_p such that $T_\tau(u)=r_p(T_\tau(c))$ in $\mathcal{E}_p$.

After identifying $\widehat{\mathbb{Z}}$ with the direct product $\prod_{p\in\mathscr{P}}\mathbb{Z}_p$ (via the Chinese Remainder Theorem), we may regard the family

$$r \coloneqq (r_p)_p$$

as an element of $\widehat{R^+}$. It is then enough for us to show that this element r belongs to the subgroup R^+ of $\widehat{R^+}$. Indeed, if true, then there is an equality $T_\tau(u)=r(T_\tau(c))$ in $\mathcal{E}_p$ for every p, and hence an equality $T_\tau(u)_{K,p}=r_K(T_\tau(c)_K)_p$ in $U'_{K,p}$ for every p and every $K\in\Omega^\circ$. It follows that, for every K, the elements $T_\tau(u)_K$ and $r_K(T_\tau(c)_K)$ of U'_K have the same image under the injective map $U'_K\to\widehat{\mathbb{Z}}\otimes_{\mathbb{Z}}U'_K$ and hence that $T_\tau(u)_K=r_K(T_\tau(c)_K)$. Since this is true for every K, it then follows that $T_\tau(u)=r(T_\tau(c))$, as required.

Now, to show that r belongs to R^+, we note first that, for every field $K\in\Omega^\circ$, Proposition (2.4) (iii) implies the existence of an element q_K of $\mathbb{Q}[\Gamma^+_K]$ such that $T_\tau(u_K)=q_K(T_\tau(c_K))$ in $\mathbb{Q}\otimes_{\mathbb{Z}}U'_K$. The resulting equalities $r_{p,K}(T_\tau(c_K)_p)=q_K(T_\tau(c_K)_p)$ in $\mathbb{Q}_p\otimes_{\mathbb{Z}}U'_K$ then combine with Proposition (2.4) to imply that, for every p, the element $q_K - r_{p,K}$ of $\mathbb{Q}_p[\Gamma_K^+]$ annihilates $T_\tau(c_K)_p$. In particular, if we write $\widehat{\mathbb{Q}}$ for the direct product $\prod_{p\in\mathscr{P}}\mathbb{Q}_p$ and $\widehat{I_K}$ for the annihilator $\widehat{\mathbb{Q}}\otimes_{\mathbb{Z}} I_K$ of $T_\tau(c_K)$ in the group ring $\widehat{\mathbb{Q}}[\Gamma_K^+]$, then it follows that, for every K in Ω°, one has

$$r_K \in \mathbb{Q}[\Gamma_K^+] + \widehat{I_K}.$$

Given this fact, the required containment $r \in R^+$ follows directly from the result of Lemma (2.6) below (with $\epsilon = 1$ so $R^+(\epsilon) = R^+$). This completes the proof of the equality (6).
In the sequel we regard both $\widehat{\mathbb{Z}} = \prod_{p\in\mathscr{P}}\mathbb{Z}_p$ and $\mathbb{Q}$ as subgroups of $\widehat{\mathbb{Q}}$ in the natural way

(2.6) Lemma. *Fix an idempotent $\epsilon = (\epsilon_K)_{K\in\Omega_+}$ of $\mathbb{Q}[\![\Gamma^+]\!]$ and define inverse limits*

$$R^+(\epsilon) := \varprojlim_{K\in\Omega_+}\mathbb{Z}[\Gamma_K]\epsilon_K,\ \ \widehat{R^+}(\epsilon) := \varprojlim_{K\in\Omega_+}\widehat{\mathbb{Z}}[\Gamma_K]\epsilon_K \quad \textit{and} \quad \mathbb{Q}\cdot\widehat{R^+}(\epsilon) := \varprojlim_{K\in\Omega_+}\widehat{\mathbb{Q}}[\Gamma_K]\epsilon_K,$$

all with respect to the natural projection maps. Then in $\mathbb{Q}\cdot\widehat{R^+}(\epsilon)$ one has

$$\widehat{R^+}(\epsilon)\cap\prod_{K\in\Omega_+}(\mathbb{Q}[\Gamma_K]+\widehat{I_K}) = R^+(\epsilon).$$

Proof. For each field $K\in\Omega_+$ the $\mathbb{Z}$-submodule $\mathbb{Z}[\Gamma_K]\epsilon_K$ of $\mathbb{Q}[\Gamma_K]$ is free and of finite rank. Since $\mathbb{Z} = \mathbb{Q}\cap\widehat{\mathbb{Z}}$ in $\widehat{\mathbb{Q}}$, one therefore has

$$\widehat{\mathbb{Z}}[\Gamma_K]\epsilon_K\cap\mathbb{Q}[\Gamma_K] = \widehat{\mathbb{Z}}[\Gamma_K]\epsilon_K\cap\mathbb{Q}[\Gamma_K]\epsilon_K = \mathbb{Z}[\Gamma_K]\epsilon_K.$$

in $\widehat{\mathbb{Q}}[\Gamma_K]$. To prove the claimed equality, it is therefore enough to show that if $\lambda = (\lambda_K)_K$ is any element of $\widehat{R^+}(\epsilon)$ such that $\lambda_K\in\mathbb{Q}[\Gamma_K]+\widehat{I_K}$ for all K in Ω_+, then one has $\lambda_K\in\mathbb{Q}[\Gamma_K^+]$ for all K. To prove this we argue by induction on the number of prime factors of $m(K)$.
If, firstly, $m(K)$ is a prime power, then the idempotent e_K is (by definition) equal to 1 and so Proposition (2.4) (i) implies that I_K, and hence also $\widehat{I_K}$, vanishes. In the case therefore the given assumptions imply directly that λ_K belongs to $\mathbb{Q}[\Gamma_K]$, as required.
Now assume to be given a natural number n and suppose that for every field K in Ω_+ such that $m(K)$ is divisible by at most n primes, one has $\lambda_K\in\mathbb{Q}[\Gamma_K]$. We fix a field F in Ω_+ such that $m(F)$ is divisible by $n+1$ primes and, for ψ in Γ_F^*, we write F_ψ for the fixed field of F under $\ker(\psi)$. Then, for each subfield E of F the subset $\Xi(E)$ of Γ_F^* comprising ψ for which $F_\psi = E$ is a (possibly empty) conjugacy class for the action of Γ on Γ_F^* and so the associated idempotent $\varepsilon_E := \sum_{\psi\in\Xi(E)}e_\psi$ belongs to $\mathbb{Q}[\Gamma_F]$.
To investigate λ_F we use the decomposition

$$\lambda_F = 1\cdot\lambda_F = \big(\sum_{\psi\in\Xi}e_\psi\big)\cdot\lambda_F = \sum_{\psi\in\Xi}e_\psi\lambda_F = \sum_{\psi\in\Xi}e_\psi\lambda_{F_\psi} = \sum_E\big(\sum_{\psi\in\Xi(E)}e_\psi\lambda_E\big) = \sum_E\varepsilon_E\lambda_E,\quad (12)$$

where the fourth equality is valid as $\lambda\in\widehat{R^+}(\epsilon)$, and in the sum E runs over all subfields of F.
Fix a subfield E of F. If $m(E)$ is divisible by fewer primes than $m(F)$ then, by hypothesis, one has $\lambda_E\in\mathbb{Q}[\Gamma_E]$. On the other hand, if $m(E)$ is divisible by the same number of primes as $m(F)$, and $r_F\in\mathbb{Q}[\Gamma_F]$ and $i_F\in\widehat{I_F}$ are such that $\lambda_F = r_F + i_F$, then one has

$$\varepsilon_E\lambda_E = \sum_{\psi\in\Xi(E)}e_\psi\lambda_E = \sum_{\psi\in\Xi(E)}e_\psi\lambda_F = \sum_{\psi\in\Xi(E)}e_\psi(r_F+i_F) = \sum_{\psi\in\Xi(E)}e_\psi r_F = \varepsilon_E r_F.$$

Here the fourth equality is valid since, under the present hypothesis, each ψ in $\Xi(E)$ cannot be trivial on the decomposition group of any prime divisor of $m(F)$ so that one has $e_\psi = e_\psi e_F$ (by Proposition (2.4) (ii)) and hence also $e_\psi(i_F) = 0$ as a consequence of Proposition (2.4) (i). These observations imply that the element $\varepsilon_E\lambda_E$ belongs to $\mathbb{Q}[\Gamma_E]$ for every subfield E of F and hence, via the decomposition (12), that λ_F belongs to $\mathbb{Q}[\Gamma_F]$. □

2.4 The proof of Coleman's Conjecture

In this section we prove Coleman's Conjecture on circular distributions and thereby complete the proof of Theorem (1.1). To state the conjecture, we write μ^* for the set of non-trivial roots of unity in $\mathbb{Q}^{\mathrm{ab}}$, and recall that a circular distribution is a Γ-equivariant function $f\colon \mu^* \to \mathbb{Q}^{\mathrm{ab},\times}$ such that, for all natural numbers n, one has

$$\prod_{\xi^n=\eta} f(\xi) = f(\eta) \quad \text{for all } \eta \in \mu^* \tag{13}$$

and, in addition, for all primes ℓ that do not divide n, the values $f(e^{2\pi i/\ell n})$ and $f(e^{2\pi i/n})$ are congruent modulo all ℓ-adic primes of $\mathbb{Q}(\ell n)$ (this last condition makes sense since (13) implies that f satisfies an analogue of the condition (2)).

Explicit examples include the 'cyclotomic distribution' Φ_{cyc} and the 'parity distribution' Φ_{par} that respectively send each $e^{2\pi i/n}$ with $n > 1$ to $1-e^{2\pi i/n}$ and to $(-1)^{\pi(n)}$, where $\pi(n)$ is defined to be 1 if n is even and -1 if it is odd. Further, the collection $\mathfrak{F}^{\mathrm{cd}}$ of circular distributions is a group under (pointwise) multiplication and has a natural action of $\mathbb{Z}[\![\Gamma]\!]$ (which we write additively), and Coleman has conjectured that

$$\mathfrak{F}^{\mathrm{cd}} = \mathbb{Z}[\![\Gamma]\!] \cdot \{\Phi_{\mathrm{cyc}}, \Phi_{\mathrm{par}}\}. \tag{14}$$

This striking conjecture was motivated by the archimedean characterization of circular units that Coleman had obtained in [Col85] and was therefore related to attempts to understand a globalised version of the theory of Coleman power series.

The next result implies that the equality (14) is valid if the $\mathbb{Z}[\![\Gamma]\!]$-module $\mathcal{E}^{\mathrm{cong}}$ is generated by the systems c and u_{odd}. This shows that Coleman's Conjecture follows from the equation (6) proved in the last section, and hence completes the proof of Theorem (1.1).

(2.7) Lemma. *There exists an isomorphism of $\mathbb{Z}[\![\Gamma]\!]$-modules $\kappa\colon \mathfrak{F}^{\mathrm{cd}} \to \mathcal{E}^{\mathrm{cong}}$ with the property that $\kappa(\Phi_{\mathrm{cyc}}) = c$ and $\kappa(\Phi_{\mathrm{par}}) = u_{\mathrm{odd}}$.*

Proof. For f in $\mathfrak{F}^{\mathrm{cd}}$, one obtains an element $u_f = (u_{f,K})_K$ of $\prod_{K\in\Omega^\circ} K^\times$ by setting

$$u_{f,K} := \mathrm{N}_{\mathbb{Q}(m(K))/K}(f(e^{2\pi i/m(K)}))$$

for all K in Ω°. We also note that, for each u in $\mathcal{E}$, there exists a unique Γ-equivariant function $f_u\colon \mu^* \to \mathbb{Q}^{\mathrm{ab},\times}$ that, at each $n > 1$, satisfies

$$f_u(e^{2\pi i/n}) := \begin{cases} u_{\mathbb{Q}(n)}, & \text{if } n \not\equiv 2 \pmod 4,\\ (1-\mathrm{Frob}_2)(u_{\mathbb{Q}(n/2)}), & \text{if } n \equiv 2 \pmod 4 \text{ and } n > 2,\\ 1, & \text{if } n = 2.\end{cases}$$

Then, by explicit computation, one verifies that every family u_f belongs to $\mathcal{E}^{\mathrm{cong}}$, that the function f_u belongs to $\mathfrak{F}^{\mathrm{cd}}$ if u belongs to $\mathcal{E}^{\mathrm{cong}}$, that the assignments $f \mapsto u_f$ and $u \mapsto f_u$ respect the actions of $\mathbb{Z}[\![\Gamma]\!]$ and that, for every f and u, there is an equality of functions $f = f_{u_f}$ and an equality of families $u = u_{f_u}$.

The required isomorphism κ is therefore obtained by setting $\kappa(f) := u_f$ for each f in $\mathfrak{F}^{\mathrm{cd}}$. □

(2.8) Remark. The above proof of Theorem (1.1) also directly implies an affirmative answer to the 'Guess' formulated by the fourth author in [Seo06, § 3], and thereby proves a distribution-theoretic analogue of the main result of Coleman in [Col85]. In addition, the discussion of [Seo08, § 1] shows that the equality (6) combines with results of Sinnott [Sin80] concerning cyclotomic units to imply that, for each n, the order of the graded module of 'truncated Euler systems' over the real abelian field $\mathbb{R} \cap \mathbb{Q}(n)$ is equal to the class number of $\mathbb{R} \cap \mathbb{Q}(n)$, as conjectured in [Seo08].

3 Non-cyclotomic Euler systems and the proof of Theorem (1.2)

In this section we introduce an explicit, inductive construction of Euler systems and, by combining this with results from § 2, are able to prove the following result.

(3.1) Theorem. *The following claims are valid.*

(i) For every $u \in \mathcal{E}$ and every $K \in \Omega^\circ$ one has $u_K \in \mathbb{Z}[\Gamma_K]\cdot c_K$.

(ii) One has $\mathrm{im}(\mathrm{Ord}_{\mathbb{Q}}) \subseteq \Theta$ and there exists an exact sequence of $\mathbb{Z}[\![\Gamma]\!]$-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{T}+\mathcal{C} \arrow[r, "\subseteq"] & \mathcal{E} \arrow[r, "\mathrm{Ord}'_{\mathbb{Q}}"] & \Theta/\varpi(\mathbb{Z}) \arrow[r] & \mathrm{cok}(\mathrm{Ord}'_{\mathbb{Q}}) \arrow[r] & 0 \end{tikzcd}$$

in which $\mathrm{Ord}'_{\mathbb{Q}}$ is the map induced by $\mathrm{Ord}_{\mathbb{Q}}$ and the exponent of $\mathrm{cok}(\mathrm{Ord}'_{\mathbb{Q}})$ divides 2.

(iii) The $\mathbb{Z}[\![\Gamma]\!]$-module $\mathcal{E}/(\mathcal{T}+\mathcal{C})$ cannot be generated by finitely many elements.

This result implies that, whilst every system in $\mathcal{E}$ is 'cyclotomic-valued' (by claim (i)) , the cyclotomic systems themselves account for a very small proportion of the full module of Euler systems in this setting (by claim (iii)). It also has the following specific consequence.

(3.2) Corollary. *Theorem (1.2) is valid.*

Proof. Theorem (3.1)(ii) implies the existence of an exact commutative diagram of R-modules

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{T}+\mathcal{C} \arrow[r] \arrow[d, two heads] & \mathcal{E} \arrow[r] \arrow[d, "\mathrm{Ord}_{\mathbb{Q}}"] & \mathcal{E}/(\mathcal{T}+\mathcal{C}) \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & \mathbb{Z} \arrow[r, "\varpi"] & \Theta \arrow[r] & \Theta/\varpi(\mathbb{Z}) \arrow[r] & 0. \end{tikzcd}$$

Here both rows are tautological, the right hand vertical map is injective (and induced by $\mathrm{Ord}'_{\mathbb{Q}}$) and the left hand vertical map is surjective since for all $t \in \mathcal{T}$ and $r = (r_K)_{K\in\Omega} \in R$ one has $\mathrm{Ord}_{\mathbb{Q}}(t + r(c)) = r_{\mathbb{Q}} \cdot \mathrm{Ord}(c) = \varpi(r_{\mathbb{Q}}) \in \varpi(\mathbb{Z})$.

This diagram implies that the cokernel of $\mathrm{Ord}_{\mathbb{Q}}$ is isomorphic to the cokernel of $\mathrm{Ord}'_{\mathbb{Q}}$ (and hence has exponent dividing 2), that $\mathcal{T}+\mathcal{C}$ is the full pre-image of $\mathbb{Z}$ under $\mathrm{Ord}_{\mathbb{Q}}$ and that $\ker(\mathrm{Ord}_{\mathbb{Q}}) = \mathcal{T} + \mathcal{C}^0$, with $\mathcal{C}^0$ the submodule of $\mathcal{C}$ comprising all systems $r(c)$ for which $\mathrm{Ord}_{\mathbb{Q}}(r(c)) = r_{\mathbb{Q}} \cdot \mathrm{Ord}_{\mathbb{Q}}(c) = \varpi(r_{\mathbb{Q}})$, and hence also $r_{\mathbb{Q}}$, vanishes.

This verifies all assertions of Theorem (1.2). □

The proof of Theorem (3.1) will occupy the remainder of this section.

3.1 Preliminary steps

In the sequel we use the idempotent $\overline{e_{\mathbf{1}}} := \big(1 - e_{\mathbf{1}_K}\big)_{K\in\Omega_+}$ of $\mathbb{Q}[\![\Gamma^+]\!]$, where $\mathbf{1}_K$ denotes the trivial character of Γ_K, and write

$$R^+_{\mathbf{1}} := R^+(\overline{e_{\mathbf{1}}}) \quad \text{and} \quad \widehat{R^+_{\mathbf{1}}} := \widehat{R^+}(\overline{e_{\mathbf{1}}})$$

for the associated rings defined in Lemma (2.6). For each K in Ω we also set

$$T_K := \sum_{\gamma\in\Gamma_K} \gamma \in \mathbb{Z}[\Gamma_K].$$

(3.3) Lemma. *For any system u in $\mathcal{E}$ there exists a unique element*

$$q_u := (q_{u,K})_{K\in\Omega_+}$$

of $R^+_{\mathbf{1}}$ that has both of the following properties:

(i) For every $K \in \Omega$ one has $(1 - e_{\mathbf{1}_K}) \cdot T_\tau(u_K) = q_{u,K} \cdot T_\tau(c_K)$ in $\mathbb{Q} \otimes_{\mathbb{Z}} T_\tau(U_K)$.

(ii) Fix a prime p and, for each natural number n, set $K_n = K_{p,n} := \mathbb{Q}(p^n)^+$. Then there exists an element

$$r_{u,p} = (r_{u,p,n})_n \in \varprojlim_{n\in\mathbb{N}} \mathbb{Z}[\Gamma_{K_n}]$$

such that, for every n, one has both

$$q_{u,K_n} = r_{u,p,n}\cdot(1-e_{\mathbf{1}_{K_n}}) \in \mathbb{Q}[\Gamma_{K_n}] \quad \textit{and} \quad u_{K_n} = r_{u,p,n}(c_{K_n}) \in U_{K_n}.$$

Proof. At the outset we note Propositions (2.2) and (2.3) (a) combine to imply that, for every prime p, there exists an element $x_{u,p} = (x_{u,p,K})_{K\in\Omega_+}$ of R_p^+ such that $T_\tau(u - x_{u,p}(c))$ is a Γ-invariant system in $\mathcal{E}_p$. Setting $u' := \overline{e_{\mathbf{1}}}(u) \in \mathcal{E}_{\mathbb{Q}}$, the element

$$q_{u,p} := \overline{e_{\mathbf{1}}}\cdot x_{u,p} \in R^+_{p,\mathbf{1}}$$

is therefore such that $q_{u,p}\cdot T_\tau(c) = T_\tau(u')$ in $T_\tau(\mathcal{E}_{\mathbb{Q}_p})$. We claim that $q_{u,p}$ is the unique element of $\mathbb{Q}_p[\![\Gamma^+]\!]$ with this property. To see this, we note that if $q' = (q'_K)_K$ is any other such element, then $(q_{u,p} - q')\cdot T_\tau(c)$ vanishes in $\mathcal{E}_{\mathbb{Q}_p}$. Hence, we must show this equality implies $q_{u,p,K} = q'_K$ for every $K \in \Omega_+$. For each such K it is thus enough to prove that, for every non-trivial χ in Γ_K^*, one has $e_\chi\cdot(q_{u,p,K} - q'_K) = 0$, or equivalently $e_\chi\cdot(q_{u,p,K_\chi} - q'_{K_\chi}) = 0$ where K_χ is the fixed field of K by $\ker(\chi)$. However, the latter equality is true since $(q_{u,p,K_\chi} - q'_{K_\chi})\cdot T_\tau(c_{K_\chi})$ vanishes, whilst Proposition (2.4) (i) implies that $e_\chi(T_\tau(c_{K_\chi}))$ is non-zero.

We next use the identifications $\widehat{\mathbb{Z}}[\Gamma_K](1-e_{\mathbf{1}_K}) = \prod_{p\in\mathscr{P}}\mathbb{Z}_p[\Gamma_K](1-e_{\mathbf{1}_K})$ for each $K\in\Omega_+$, to deduce the existence of an element

$$q_u = (q_{u,K})_{K\in\Omega_+} \in \widehat{R^+_{\mathbf{1}}}$$

with $q_{u,K} = (q_{u,p,K})_{p\in\mathscr{P}}$ for all K. In addition, for each such K, Proposition (2.4) (iii) implies the existence of an element y_K of $\mathbb{Q}[\Gamma_K]$ with $T_\tau(u_K) = y_K\cdot T_\tau(c_K)$ in $\mathbb{Q}\otimes_{\mathbb{Z}} T_\tau(U_K)$ and so

$$(q_{u,K} - (1-e_{\mathbf{1}_K})y_K)\cdot T_\tau(c_K) = T_\tau(u'_K) - (1-e_{\mathbf{1}_K})y_K\cdot T_\tau(c_K) = 0$$

in $\widehat{\mathbb{Q}}\otimes_{\mathbb{Z}} T_\tau(U_K)$. This equality implies that $q_{u,K}$ belongs to $\mathbb{Q}[\Gamma_K] + \widehat{I_K}$, where the module $\widehat{I_K}$ is defined in the proof of Lemma (2.5). In particular, since this containment is true for every K, we may apply Lemma (2.6) (with $\epsilon = \overline{e_{\mathbf{1}}}$) to deduce q_u belongs to the subgroup $R^+_{\mathbf{1}}$ of $\widehat{R^+_{\mathbf{1}}}$. In addition, for every $K\in\Omega_+$ one has

$$(1-e_{\mathbf{1}_K})\cdot T_\tau(u_K) = T_\tau(u'_K) = q_{u,K}\cdot T_\tau(c_K),$$

and so this element q_u has the property described in claim (i).

We must now show that q_u has the property described in claim (ii). To do this we fix a prime p, a natural number n such that $K_n \neq \mathbb{Q}$ and an element $\widetilde{q}_{u,n}$ of $\mathbb{Z}[\Gamma_{K_n}]$ with $\widetilde{q}_{u,n}(1-e_{\mathbf{1}_{K_n}}) = q_{u,K_n}$. Then, since the element $v_n := \widetilde{q}_{u,n}(c_{K_n}) - u_{K_n}$ belongs to the torsion-free group $T_\tau(U_{\mathbb{Q}(p^n)})$ and is annihilated by $1-e_{\mathbf{1}_{K_n}}$ (when regarded as an element of $\mathbb{Q}\otimes_{\mathbb{Z}} T_\tau(U_{\mathbb{Q}(p^n)})$), it is fixed by every element of Γ_{K_n} and so belongs to the subgroup $\mathbb{Q}^\times \cap T_\tau(U_{\mathbb{Q}(p^n)})$ of $\mathbb{Q}^\times$. Since the latter subgroup is generated by p, one therefore has $v_n = y_{u,p,n}\cdot p$ for some $y_{u,p,n}\in\mathbb{Z}$ and hence also

$$\widetilde{q}_{u,n}(c_{K_n}) - u_{K_n} = y_{u,p,n}\cdot p = y_{u,p,n}\cdot \mathrm{N}_{K_n/\mathbb{Q}}(c_{K_n}).$$

The element $r_{u,p,n} := \widetilde{q}_{u,n} - y_{u,p,n}\cdot T_{K_n}$ of $\mathbb{Z}[\Gamma_{K_n}]$ is therefore such that $u_{K_n} = r_{u,p,n}(c_{K_n})$ and $r_{u,p,n}(1-e_{\mathbf{1}_{K_n}}) = q_{u,K_n}$. Hence, to prove claim (ii), it is enough to show that the family

$$r_{u,p} := (r_{u,p,n})_n \in \prod_{n\in\mathbb{N}}\mathbb{Z}[\Gamma_{K_n}]$$

belongs to $\varprojlim_n \mathbb{Z}[\Gamma_{K_n}]$. To do this, we note that, by Proposition (2.4) (i), the element c_{K_n} generates a free $\mathbb{Z}[\Gamma_{K_n}]$-module of rank one, and hence that it suffices to show that the element $r_{u,p,n} - \pi_{K_{n+1}/K_n}(r_{u,p,n+1})$ of $\mathbb{Z}[\Gamma_{K_n}]$ annihilates c_{K_n}. This in turn follows directly from the distribution relations

$$\begin{aligned} r_{u,p,n}(c_{K_n}) = u_{K_n} &= \mathrm{N}_{K_{n+1}/K_n}(u_{K_{n+1}}) = \mathrm{N}_{K_{n+1}/K_n}(r_{u,p,n+1}(c_{K_{n+1}})) \\ &= \pi_{K_{n+1}/K_n}(r_{u,p,n+1})(\mathrm{N}_{K_{n+1}/K_n}(c_{K_{n+1}})) = \pi_{K_{n+1}/K_n}(r_{u,p,n+1})(c_{K_n}). \qquad \square \end{aligned}$$

The key to our investigation of the elements q_u that are provided by Lemma (3.3) is provided by the following exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R^+ \arrow[r, "\cdot\overline{e_{\mathbf{1}}}"] \arrow[d] & R^+_{\mathbf{1}} \arrow[r, "\delta"] \arrow[d] & \varprojlim^1_{K\in\Omega_+} (\mathbb{Z}\cdot T_K) \arrow[r] \arrow[d, "\omega"] & 0 \\
0 \arrow[r] & \prod_{p\in\mathscr{P}} R^+(p) \arrow[r, "\cdot\overline{e_{\mathbf{1}}}"] & \prod_{p\in\mathscr{P}} R^+_{\mathbf{1}}(p) \arrow[r, "(\delta^{(p)})_p"] & \prod_{p\in\mathscr{P}} \varprojlim^1_n (\mathbb{Z}\cdot T_{\mathbb{Q}(p^n)^+}) \arrow[r] & 0,
\end{tikzcd} \tag{15}$$

where for each p we set

$$R^+(p) := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}[\Gamma^+_{\mathbb{Q}(p^n)}] \quad\text{and}\quad R^+_{\mathbf{1}}(p) := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}[\Gamma^+_{\mathbb{Q}(p^n)}](1-e_{\mathbf{1}_{\mathbb{Q}(p^n)^+}}).$$

The upper exact sequence in this diagram is obtained by combining the long exact sequence of R^+-modules that is induced by passing to the limit over $K\in\Omega_+$, with respect to projection maps induced by $\pi_{L/K,\mathbb{Q}}$ for $K\subseteq L$, of the obvious exact sequences

$$0\to\mathbb{Z}\cdot T_K \xrightarrow{\subseteq} \mathbb{Z}[\Gamma_K] \xrightarrow{x\mapsto x(1-e_{\mathbf{1}_K})} \mathbb{Z}[\Gamma_K](1-e_{\mathbf{1}_K})\to 0 \tag{16}$$

with the following facts: the limit $\varprojlim_{K\in\Omega_+}\mathbb{Z}\cdot T_K$ vanishes since $\pi_{L/K}(T_L)=[L:K]\cdot T_K$ for $K\subseteq L$ and the derived limit $\varprojlim^1_{K\in\Omega_+}\mathbb{Z}[\Gamma_K]$ vanishes as a consequence of the Mittag–Leffler criterion since the transition maps $\pi_{L/K}$ are surjective. In a similar way, the lower exact sequence in the diagram is the direct product over p of the exact sequences derived by passing to the inverse limit over n of the exact sequences (16) with $K=\mathbb{Q}(p^n)^+$. Finally, we note that all of the vertical maps in (15) are the natural (diagonal) projection maps.

In the next result we provide an explicit description of the connecting homomorphism δ and projection map ω that occur in (15). For each natural number m we set

$$\varphi(m) := [\mathbb{Q}(m)^+ : \mathbb{Q}] \quad\text{and}\quad \mathbb{Z}_{/m} := \mathbb{Z}/(m\mathbb{Z}).$$

(3.4) Lemma. *The following claims are valid.*

(i) There exists a natural isomorphism

$$\varprojlim^1_{K\in\Omega_+} (\mathbb{Z}\cdot T_K) \cong \big(\varprojlim_m \mathbb{Z}_{/\varphi(m)}\big)/\mathbb{Z}$$

where $\mathbb{Z}$ is embedded diagonally in the stated limit. The induced composite map

$$\delta' \colon \varprojlim_{K\in\Omega_+} \mathbb{Z}[\Gamma_K](1-e_{\mathbf{1}_K}) \xrightarrow{\delta} \varprojlim^1_{K\in\Omega_+} (\mathbb{Z}\cdot T_K) \xrightarrow{\simeq} \big(\varprojlim_m \mathbb{Z}_{/\varphi(m)}\big)/\mathbb{Z}$$

sends each element $q=(q_K)_K$ of $\varprojlim_{K\in\Omega_+}\mathbb{Z}[\Gamma_K](1-e_{\mathbf{1}_K})$ to the family

$$\delta'(q) := \big(\pi_{\mathbb{Q}(m)^+/\mathbb{Q}}(q_m) \mod \varphi(m)\big)_{m\in\mathbb{N}},$$

where q_m is any choice of element of $\mathbb{Z}[\Gamma^+_{\mathbb{Q}(m)}]$ with $q_m\cdot(1-e_{\mathbf{1}_{\mathbb{Q}(m)^+}}) = q_{\mathbb{Q}(m)^+}$.

(ii) For each prime p, there exists a natural isomorphism

$$\varprojlim_n{}^1(\mathbb{Z}\cdot T_{\mathbb{Q}(p^n)^+}) \cong \big(\varprojlim_n \mathbb{Z}_{/\varphi(p^n)}\big)/\mathbb{Z},$$

where $\mathbb{Z}$ is embedded diagonally in the stated limit.

(iii) Write Δ for the diagonal map

$$\varprojlim_m \mathbb{Z}_{/\varphi(m)} \to \prod_{p\in\mathscr{P}} \varprojlim_n \mathbb{Z}_{/\varphi(p^n)}, \quad (a_m)_{m\in\mathbb{N}} \mapsto \big((a_{p^n})_{n\in\mathbb{N}}\big)_p.$$

Then there exists a commutative diagram

$$\begin{tikzcd}
\varprojlim\limits_{K\in\Omega_+}{}^{1} (\mathbb{Z}\cdot\mathcal{T}_K) \arrow[r, "\simeq"] \arrow[d, "\omega"] & \big(\varprojlim\limits_{m} \mathbb{Z}_{/\varphi(m)}\big)/\mathbb{Z} \arrow[d, "\overline{\Delta}"] \\
\prod\limits_{p\in\mathscr{P}} \varprojlim\limits_{n}{}^{1}(\mathbb{Z}\cdot\mathcal{T}_{\mathbb{Q}(p^n)^+}) \arrow[r, "\simeq"] & \prod\limits_{p\in\mathscr{P}} \Big(\big(\varprojlim\limits_{n} \mathbb{Z}_{/\varphi(p^n)}\big)/\mathbb{Z}\Big),
\end{tikzcd}$$

in which the horizontal maps are the isomorphisms in (i) and (ii) and $\overline{\Delta}$ is induced by Δ.

Proof. For every K in Ω_+, the exact sequence (16) lies in a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}\cdot\mathcal{T}_K \arrow[r, "\subseteq"] \arrow[d, "\theta'_K", "\simeq"'] & \mathbb{Z}[\Gamma_K] \arrow[r, "\cdot\overline{e_{\mathbf{1}}}"] \arrow[d, "\pi_{K/\mathbb{Q}}"] & \mathbb{Z}[\Gamma_K](1-e_{\mathbf{1}_K}) \arrow[r] \arrow[d, "\theta_K"] & 0 \\
0 \arrow[r] & \mathbb{Z}\cdot[K:\mathbb{Q}] \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Z}_{/[K:\mathbb{Q}]} \arrow[r] & 0,
\end{tikzcd}$$

in which θ'_K is the restriction of $\pi_{K/\mathbb{Q}}$ and so is bijective, the second vertical map is surjective and the map θ_K is induced by the commutativity of the first square and the exactness of both rows. As K varies over Ω_+, these diagrams are compatible with respect to the natural transition maps. Upon passing to the limit over K of these diagrams, and applying the Mittag–Leffler criterion to the second vertical maps, one therefore obtains an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & R^+ \arrow[r] \arrow[d] & R^+_{\mathbf{1}} \arrow[r, "\delta"] \arrow[d, "(\theta_K)_K"] & \varprojlim\limits_{K\in\Omega_+}{}^{1} (\mathbb{Z}\cdot\mathcal{T}_K) \arrow[r] \arrow[d, "\simeq"] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r] & \varprojlim\limits_{K\in\Omega_+} \mathbb{Z}_{/[K:\mathbb{Q}]} \arrow[r] & \varprojlim\limits_{K\in\Omega_+}{}^{1} (\mathbb{Z}\cdot[K:\mathbb{Q}]) \arrow[r] & 0
\end{tikzcd} \tag{17}$$

in which the first vertical map is the natural projection map and the third is induced by the isomorphisms $(\theta'_K)_K$ and so is bijective. The exactness of the diagram therefore induces an isomorphism

$$\varprojlim_{K\in\Omega_+}{}^{1} (\mathbb{Z}\cdot\mathcal{T}_K) \cong \varprojlim_{K\in\Omega_+}{}^{1} (\mathbb{Z}\cdot[K:\mathbb{Q}]) \cong \big(\varprojlim_{K\in\Omega_+} \mathbb{Z}_{/[K:\mathbb{Q}]}\big)/\mathbb{Z}$$

of the form stated in claim (i). Given this explicit construction of the isomorphism, the remaining assertion of claim (i) follows immediately from the commutative diagram (17).

In just the same way, for each prime p one can verify the assertion of claim (ii), construct a homomorphism $\theta_p\colon R^+_{\mathbf{1}}(p) \to \big(\varprojlim_n \mathbb{Z}_{/\varphi(p^n)}\big)/\mathbb{Z}$ and give an explicit description of the connecting homomorhism $\delta^{(p)}$ in (15) in terms of θ_p.

By using these explicit descriptions, it is then straightforward to verify that the map $\overline{\Delta}$ described in the statement of claim (iii) is the unique dashed arrow that renders the following diagram commutative

$$\begin{tikzcd}
0 \arrow[r] & R^+ \arrow[r, "\cdot\overline{e_{\mathbf{1}}}"] \arrow[d] & R^+_{\mathbf{1}} \arrow[r, "(\theta_K)_K"] \arrow[d] & \big(\varprojlim\limits_{K\in\Omega_+} \mathbb{Z}_{/[K:\mathbb{Q}]}\big)/\mathbb{Z} \arrow[r] \arrow[d, dashed] & 0 \\
0 \arrow[r] & \prod\limits_{p\in\mathscr{P}} R^+(p) \arrow[r, "\cdot\overline{e_{\mathbf{1}}}"] & \prod\limits_{p\in\mathscr{P}} R^+_{\mathbf{1}}(p) \arrow[r, "(\theta_p)_p"] & \prod\limits_{p\in\mathscr{P}} \Big(\big(\varprojlim\limits_{n} \mathbb{Z}_{/\varphi(p^n)}\big)/\mathbb{Z}\Big) \arrow[r] & 0.
\end{tikzcd}$$

This proves claim (iii). □

Properties of the map Δ in Lemma (3.4)(iii) will play a key role in our proof of Theorem (3.1). Before establishing these properties, we must first make several elementary observations. To do this we define a $\widehat{\mathbb{Z}}$-module by setting

$$\mathcal{U} := \Big\{ (\alpha^{(p)})_p \in \prod_{p\in\mathscr{P}} \varprojlim_n \mathbb{Z}_{(\varphi(p^n))} \mid \alpha_1^{(p)} \equiv \alpha_{m_i(p)^*}^{(\ell_i(p))} \mod \ell_i(p)^{m_i(p)} \text{ for } p > 3 \text{ and } 1 \le i \le t(p) \Big\},$$

where for each $p > 3$ we write the prime factorisation of $\varphi(p) = (p-1)/2$ as

$$\varphi(p) = \prod_{i=1}^{t(p)} \ell_i(p)^{m_i(p)} \tag{18}$$

and set $m_i(p)^* := m_i(p) + 2$ if $\ell_i(p) = 2$ (so $\varphi(p)$ is even) and $m_i(p)^* := m_i(p) + 1$ otherwise. For each natural number m we also write p_m for the m-th prime number (in ascending order).

(3.5) Lemma. *For every natural number s the following claims are valid.*

(i) Fix an element $\lambda = (\lambda_n)_n$ of $\varprojlim_n \mathbb{Z}_{(\varphi(n))}$ and a divisor t of $\varphi(s)$ with $t > 1$ and set

$$\tilde{t} := \begin{cases} t\prod_{\ell|t}\ell, & \textit{if } t \textit{ is divisible by an odd prime} \\ 4t, & \textit{otherwise,} \end{cases}$$

where ℓ runs over all prime divisors of t. Then $\lambda_s \equiv \lambda_{\tilde{t}} \mod t$. In particular, for a prime p and any index i as in (18) one has $\lambda_p \equiv \lambda_{\ell_i(p)^{m_i(p)^*}} \mod \ell_i(p)^{m_i(p)}$.

(ii) The image of Δ is contained in $\mathcal{U}$.

(iii) Let $\{\mu_{p_i} \mid 1 \le i \le s\}$ be integers with the property that

$$\mu_{p_i} \equiv \mu_{p_j} \mod p_j^{\operatorname{ord}_{p_j}(\varphi(p_i))} \quad \textit{for } 2 < i \le s \textit{ and } 1 \le j < i.$$

Then there exists an element $\alpha = (\alpha^{(p)})_p$ of $\mathcal{U}$ with both of the following properties:

(a) for every $i \in \{1, \dots, s\}$ one has $\alpha^{(p_i)} = (\mu_{p_i} \mod \varphi(p_i^n))_{n\in\mathbb{N}}$;

(b) for every prime $p > p_s$, there exists an integer μ_p with $\alpha^{(p)} = (\mu_p \mod \varphi(p^n))_{n\in\mathbb{N}}$.

Proof. The first assertion of claim (i) is valid since, for each $\lambda = (\lambda_n)_n$ in $\varprojlim_n \mathbb{Z}_{(\varphi(n))}$, there are congruences $\lambda_s \equiv \lambda_{s\tilde{t}} \equiv \lambda_{\tilde{t}} \mod t$, where the first is valid since t divides $\varphi(s)$ and the second since t divides $\varphi(\tilde{t})$. The second assertion in claim (i) is then obtained by taking $s = p$ and $t = \ell_i(p)^{m_i(p)}$.

To prove claim (ii) we fix an element $\lambda = (\lambda_n)_n$ as above and a prime $p > 3$ and use the notation introduced in (18). It is then enough to note that for each i with $1 \le i \le t(p)$ one has

$$\Delta(\lambda)_1^{(p)} \equiv \lambda_p \equiv \lambda_{\ell_i(p)^{m_i(p)^*}} \equiv \Delta(\lambda)_{m_i(p)^*}^{(\ell_i(p))} \mod \ell_i(p)^{m_i(p)}.$$

Here the second congruence follows from claim (i) and the others from the definition of Δ.

To prove claim (iii), we first construct a suitable family of integers $\{\mu_{p_N}\}_N$ by using induction on the natural number N. If $N \le s$, we take μ_{p_N} to be the integer specified in the statement. For $N > s$ we assume that suitable integers p_j have been fixed for $1 \le j < N$ and then take μ_{p_N} to be any integer that solves the simultaneous congruences

$$\mu_{p_N} \equiv \mu_{p_j} \mod p_j^{\operatorname{ord}_{p_j}(\varphi(p_N))} \quad \text{for } 1 \le j < N. \tag{19}$$

It is then clear that the image α of this family $(\mu_p)_{p\in\mathscr{P}}$ under the projection from $\prod_{p\in\mathscr{P}} \mathbb{Z}$ to $\prod_{p\in\mathscr{P}} \varprojlim_n \mathbb{Z}_{(\varphi(p^n))}$ has the stated conditions (a) and (b). To show α belongs to $\mathcal{U}$ we fix a natural number $N > 2$ and an integer i with $1 \le i \le t(p_N)$ and set $\ell := \ell_i(p_N)$, $m := m_i(p_N)$ and $m^* := m_i(p_N)^*$. It is then enough to note there are congruences modulo ℓ^m of the form

$$\alpha_1^{(p_N)} \equiv \mu_{p_N} \equiv \mu_\ell \equiv \alpha_{m^*}^{(\ell)},$$

where the first is true since ℓ^m divides $\varphi(p_N)$, the second follows from (19) and the third is true since the definition of m^* implies $\varphi(\ell^{m^*})$ is divisible by ℓ^m. □

We can now establish the key properties of the map Δ in Lemma (3.4) (iii).

(3.6) Proposition. *The following claims are valid.*

(i) Δ is injective and has image equal to $\mathcal{U}$.

(ii) The kernel of $\overline{\Delta}$ is isomorphic to $\Theta/\varpi(\mathbb{Z})$ and is non-trivial.

Proof. To show Δ is injective we fix an element $\lambda = (\lambda_n)_n$ in its kernel. We also fix a natural n and write $\prod_{i=1}^{t} \ell_i^{m_i}$ for the prime factorisation of $\varphi(n)$. Then, for each i, there are congruences modulo $q_i := \ell_i^{m_i}$ of the form $\lambda_n \equiv \lambda_{\tilde{q}_i} \equiv 0$, where the first follows from Lemma (3.5) (i) and the second is valid since $\lambda \in \ker(\Delta)$ and q_i divides $\varphi(\tilde{q}_i)$. By the Chinese Remainder Theorem, it therefore follows that $\lambda_n \equiv 0 \mod \varphi(n)$ and, since n is an arbitrary natural number, this implies λ vanishes, as required to prove injectivity of Δ.

To prove $\mathrm{im}(\Delta) = \mathcal{U}$ it suffices, in view of Lemma (3.5) (i), to construct a pre-image under Δ of an arbitrary element $(\alpha^{(p)})_p$ of $\mathcal{U}$. To do this, we regard α as fixed and, for each natural number n, define λ_n to be the unique solution (in $\mathbb{Z}_{(\varphi(n))}$) to the family of congruences

$$\lambda_n \equiv \alpha^{\ell_i}_{m_i+a(\ell_i)} \mod \ell_i^{m_i} \quad \text{for all } 1 \leq i \leq t, \tag{20}$$

where $\prod_{i=1}^{t} \ell_i^{m_i}$ is the prime factorisation of $\varphi(n)$ and for each prime ℓ we set $a(\ell) := 2$ if $\ell = 2$ and $a(\ell) := 1$ otherwise (so that $\ell_i^{m_i}$ divides $\varphi(\ell_i^{m_i+a(\ell_i)})$).

We claim first that $\lambda_{p^s} = \alpha^{(p)}_s$ for every prime p and natural number s (such that $\varphi(p^s) \neq 1$). If $p \in \{2, 3\}$, this follows easily from the fact p is the only prime divisor of $\varphi(p^s)$. If $p > 3$, then it is true since, in terms of the notation in (18), one has $\varphi(p^s) = p^{s-1} \prod_{i=1}^{t(p)} \ell_i(p)^{m_i(p)}$ and so λ_{p^s} is the unique solution of the congruences

$$\begin{aligned} &\lambda_{p^s} \equiv \alpha^{(p)}_s \mod p^{s-1}, \\ &\lambda_{p^s} \equiv \alpha^{(\ell_i(p))}_{m_i(p)^*} \equiv \alpha^{(p)}_1 \equiv \alpha^{(p)}_s \mod \ell_i^{m_i(p)} \quad \text{for all } 1 \leq i \leq t(p). \end{aligned}$$

Here the second of the lower congruences follows from the definition of $\mathcal{U}$ and the third is true since $\alpha^{(p)} \in \varprojlim_n \mathbb{Z}_{(\varphi(p^n))}$. To conclude the proof of claim (i) it is thus enough to show λ belongs to $\varprojlim_n \mathbb{Z}_{(\varphi(n))}$ (since then the above observations imply $\Delta(\lambda) = (\alpha^{(p)})_p$). To do this we must show that for all $m \in \mathbb{N}$ and all divisors n of m (with $\varphi(n) \neq 1$) one has $\lambda_m \equiv \lambda_n \mod \varphi(n)$. With $\prod_{i=1}^{t} \ell_i^{m_i}$ denoting the prime factorisation of $\varphi(n)$ (as above), it is therefore enough, by the Chinese Remainder Theorem, to prove for each $i \in \{1, \ldots, t\}$ that $\lambda_m \equiv \lambda_n \mod \ell_i^{m_i}$. For each i we set $z_i := \mathrm{ord}_{\ell_i}(\varphi(m))$ and note $m_i \leq z_i$ as $\varphi(n)$ divides $\varphi(m)$. Then the definition of λ_m via (20) (with n replaced by m) implies that $\lambda_m \equiv \alpha^{(\ell_i)}_{z_i+a(\ell_i)} \mod \ell_i^{z_i}$ and hence, since $\alpha^{(\ell_i)} \in \varprojlim_{b \in \mathbb{N}} \mathbb{Z}_{(\varphi(\ell_i^b))}$, that

$$\lambda_m \equiv \alpha^{(\ell_i)}_{z_i+a(\ell_i)} \equiv \alpha^{(\ell_i)}_{m_i+a(\ell_i)} \equiv \lambda_n \mod \ell_i^{m_i},$$

where the last congruence follows from the definition of λ_n via (20). This proves claim (i).

The above argument also shows that the (injective) map Δ induces an isomorphism between $\ker(\overline{\Delta})$ and the quotient $\Theta/\varpi(\mathbb{Z})$. To prove claim (ii), it is therefore enough to construct a non-zero element in $\ker(\overline{\Delta})$. To do this we first apply Lemma (3.5) (iii) with $s = 2$, $\mu_2 = 1$ and $\mu_3 = 3$ to obtain an element $\alpha = (\alpha^p)_p$ of $\mathcal{U}$ with the following properties

(C$_1$) $\alpha^{(2)}_n \equiv 1 \bmod 2^{n-2}$ for all $n > 2$ and $\alpha^{(3)}_n \equiv 3 \bmod 3^{n-1}$ for all $n > 1$;

(C$_2$) For every $p > 3$, there exists $\mu_p \in \mathbb{Z}$ such that $\alpha^{(p)}_n \equiv \mu_p \bmod \varphi(p^n)$ for all $n > 1$.

Taking account of claim (i), we define λ to be the unique element of $\varprojlim_n \mathbb{Z}_{(\varphi(n))}$ with $\Delta(\lambda) = \alpha$ and we claim this element corresponds to a non-trivial element of $\ker(\overline{\Delta})$. To see this we note first that the image under $\overline{\Delta}$ of the class of λ is represented by the class of α and so is trivial as a direct consequence of the conditions (C$_1$) and (C$_2$). Then, to prove that the class of λ in $\big(\varprojlim_m \mathbb{Z}_{(\varphi(m))}\big)/\mathbb{Z}$ is non-trivial we argue by contradiction and so assume the existence of $\mu \in \mathbb{Z}$ such that $\lambda_n \equiv \mu \bmod \varphi(n)$ for all $n > 4$. Then condition (C$_1$) implies both that

$$\mu \equiv \lambda_{2^n} \equiv \alpha^{(2)}_n \equiv 1 \mod 2^{n-2} \quad \text{for all } n > 2,$$

(so that $\mu = 1$) and also that

$$\mu \equiv \lambda_{3^2} \equiv \alpha_2^{(3)} \equiv 0 \mod 3.$$

Since these congruences are not compatible, this concludes the proof of Proposition (3.6). □

3.2 The proof of Theorem (3.1)

For each u in $\mathcal{E}$ we use the element $q_u = (q_{u,K})_{K\in\Omega_+}$ of $R_{\mathbf{1}}^+$ constructed in Lemma (3.3) (i).
To prove claim (i) we assume (as we may) that $K = \mathbb{Q}(n)$ for a natural number $n > 5$. We recall (from [BS21, Lem. 4.3]) that in this case the group $U_K^{\tau=-1}$ is generated by $-e^{2\pi i/n} = (1-\tau)(c_K)$ and so belongs to $\mathbb{Z}[\Gamma_K]\cdot c_K$. We also note that $T_\tau(u_K)$ and $T_\tau(c_K)$ belong to the torsion-free subgroup $T_\tau(U_K)$ of U_{K^+} and we fix a lift $\widetilde{q_K}$ of q_{u,K^+} to $\mathbb{Z}[\Gamma_K]$.
We first consider the case n is divisible by two distinct prime numbers. In this case Proposition (2.4) (i) implies $T_\tau(u_K)$ and $T_\tau(c_K)$ are annihilated by $e_{\mathbf{1}}$ (when considered as elements of $\mathbb{Q}\otimes_{\mathbb{Z}} T_\tau(U_K)$). In $T_\tau(U_K)$ one therefore has

$$\begin{aligned} T_\tau(u_K - \widetilde{q_K}(c_K)) &= T_\tau(u_K) - \widetilde{q_K}(T_\tau(c_K)) \\ &= \overline{e_{\mathbf{1}}}(T_\tau(u_K)) - (\widetilde{q_K}\cdot\overline{e_{\mathbf{1}}})(T_\tau(c_K)) \\ &= q_{u,K^+}(T_\tau(c_K)) - q_{u,K^+}(T_\tau(c_K)) = 0, \end{aligned}$$

where the third equality follows from Lemma (3.3) (i). This implies $u_K - \widetilde{q_K}(c_K)$ belongs to $U_K^{\tau=-1}$ and hence, by the observation above, that u_K belongs to $\mathbb{Z}[\Gamma_K]\cdot c_K$.
We assume next that $n = p^t$ for a prime p and natural number t. In this case there exists an integer m with $\mathrm{N}_{K/\mathbb{Q}}(u_K) = p^m = \mathrm{N}_{K/\mathbb{Q}}(c_K)^m$ and so, after replacing u by $u - m\cdot c$, we can assume $T_\tau(u_K)$ is annihilated by $e_{\mathbf{1}_{K^+}}$. Then in $T_\tau(U_K)$ one has

$$T_\tau(u_K) = (1 - e_{\mathbf{1}_{K^+}})(u_{K^+}) = (1 - e_{\mathbf{1}_{K^+}})r_{u,p,t}(c_{K^+}) = q_{u,K^+}(c_{K^+}) = T_\tau(\widetilde{q_K}(c_K)),$$

where the second and third equalities follow from Lemma (3.3) (ii). It follows that $u_K - \widetilde{q_K}(c_K)$ belongs to $U_K^{\tau=-1}$ and, by the same argument as above, this implies $u_K \in \mathbb{Z}[\Gamma_K]\cdot c_K$ and so completes the proof of claim (i).
To prove claim (ii), we consider the composite homomorphism

$$\mathcal{E}/(\mathcal{T}+\mathcal{C}) \xrightarrow{u\mapsto T_\tau(u)} T_\tau(\mathcal{E})/T_\tau(\mathcal{C}) \xrightarrow{T_\tau(u)\mapsto\delta(q_u)} \ker(\omega) \cong \ker(\overline{\Delta}), \tag{21}$$

where ω and δ are the maps that occur in the diagram (15) and the isomorphism is induced by the diagram in Lemma (3.4) (iii). Lemma (2.5) implies that the first map in this composite is bijective. The second map is well-defined since the property of q_u described in Lemma (3.3) (ii) combines with a diagram chase of (15) to imply $\delta(q_u) \in \ker(\omega)$ for every $u \in \mathcal{E}$. The latter map is also injective since if $\delta(q_u)$ vanishes, then the upper row of (15) implies the existence of an element r of R^+ such that, for all $K \in \Omega_+^\circ$, one has $r_K(1 - e_{\mathbf{1}_K}) = q_{u,K}$ and hence, by Lemma (3.3) (i), $T_\tau(u_K) - r_K(T_\tau(c_K))$ belongs to $T_\tau(U_K)^{\Gamma_K}$ and so is a strictly positive rational number: this last fact implies $T_\tau(u_K) = r_K(T_\tau(c_K))$ for all K (this is clear if $m(K)$ is not a prime power and, if $m(K)$ is a power of p, follows from the norm coherency of $T_\tau(u_L) - r_L(T_\tau(c_L))$ as L varies over fields of p-power conductor) and hence that $T_\tau(u) = r(T_\tau(c)) \in T_\tau(\mathcal{C})$, as required.
We next claim that, after using Proposition (3.6) (ii) to identify $\ker(\overline{\Delta})$ with $\Theta/\varpi(\mathbb{Z})$, the map (21) sends each u to the class represented by $\mathrm{Ord}_{\mathbb{Q}}(u) = (\mathrm{ord}_p(u))_p$. This follows from an explicit computation of the connecting homomorphism δ and the fact that for every p and every natural number n one has

$$\begin{aligned} \mathrm{ord}_p\big(\mathrm{N}_{\mathbb{Q}(p^n)/\mathbb{Q}}(u_{\mathbb{Q}(p^n)})\big) &= \mathrm{ord}_p\big(\mathrm{N}_{\mathbb{Q}(p^n)^+/\mathbb{Q}}(T_\tau(u_{\mathbb{Q}(p^n)}))\big) = \mathrm{ord}_p\big(\mathrm{N}_{\mathbb{Q}(p^n)^+/\mathbb{Q}}(T_\tau(r_{u,p,n}(c_{\mathbb{Q}(p^n)})))\big) \\ &= r_{u,p,0}\cdot\mathrm{ord}_p\big(\mathrm{N}_{\mathbb{Q}(p^n)/\mathbb{Q}}(c_{\mathbb{Q}(p^n)})\big) = r_{u,p,0}\cdot\mathrm{ord}_p(p) = r_{u,p,0}, \end{aligned}$$

with $r_{u,p,n}$ the element of $\mathbb{Z}[\Gamma^+_{\mathbb{Q}(p^n)}]$ defined in Lemma (3.3) (ii) and $r_{u,p,0}$ its projection to $\mathbb{Z}$.
To complete the proof of claim (ii), it is now enough to prove the exponent of the cokernel of the second map in (21) divides 2. To do this we fix an element $q = (q_K)_{K\in\Omega^+}$ of $R_{\mathbf{1}}^+$ with

$\delta(q) \in \ker(\omega)$. Then, by chasing through the diagram (15), one finds that, for each prime p, there exists a unique element μ_p of $\varprojlim_{n\in\mathbb{N}} \mathbb{Z}[\Gamma^+_{\mathbb{Q}(p^n)}]$ with $q_K = (1 - e_{\mathbf{1}_K})\mu_{p,K}$ for every $K = \mathbb{Q}(p^n)^+$. For each $K \in \Omega$ we now define an element of U_K by setting

$$u_K := \begin{cases} q_{K^+}(T_\tau(c_K)) & \text{if } m(K) \text{ is divisible by two distinct primes,} \\ \mu_{p,K^+}(T_\tau(c_K)) & \text{if } m(K) = p^n \text{ for some prime } p. \end{cases}$$

We claim that the family $u = (u_K)_{K\in\Omega^\circ}$ satisfies the distribution relation (1) for all $K \subset L$ and so belongs to $\mathcal{E}$. This is clear if $m(K)$ and $m(L)$ are either both composite or both prime powers since c validates (1), $\pi_{L^+/K^+}(q_{L^+}) = q_{K^+}$ and $\pi_{L^+/K^+}(\mu_{p,L^+}) = \mu_{p,K^+}$ if $m(L)$ is a power of p. We can thus assume $m(L)$ is composite and $K = \mathbb{Q}(p^n)$ for a prime p and natural number n. In this case the set $S(L/K)$ of primes ramifying in L but not K is non-empty and so the element $P_{L/K} := \prod_{\ell\in S(L/K)}(1 - \mathrm{Frob}_\ell^{-1})$ of $\mathbb{Z}[\Gamma_K]$ is annihilated by $e_{\mathbf{1}_K}$. One then derives the required distribution relation via the computation

$$\begin{aligned} \mathrm{N}_{L/K}(u_L) = \mathrm{N}_{L/K}(q_L \cdot T_\tau(c_L)) &= q_{K^+} \cdot T_\tau(\mathrm{N}_{L/K}(c_L)) = q_{K^+} \cdot P_{L/K}(T_\tau(c_K)) \\ &= \mu_{p,K^+} \cdot P_{L/K}(T_\tau(c_K)) = P_{L/K}(u_K), \end{aligned}$$

where the third equality is true since c validates (1) and the fourth since

$$P_{L/K} \cdot \mu_{p,K^+} = P_{L/K}(1 - e_{\mathbf{1}_K}) \cdot \mu_{p,K^+} = P_{L/K} \cdot ((1 - e_{\mathbf{1}_{K^+}})\mu_{p,K^+}) = P_{L/K} \cdot q_{K^+}.$$

At this stage we know $u \in \mathcal{E}$ and hence that $2u = T_\tau(u) \in T_\tau(\mathcal{E})$. To complete the proof of claim (ii) it is therefore enough to note that $q_{2u} = 2q$ and so the second map in (21) sends the class of $T_\tau(u)$ to $2\delta(q)$.

Claim (ii) reduces claim (iii) to showing the existence of infinitely many elements of $2{\cdot}\Theta$ whose projections to $\Theta/\varpi(\mathbb{Z})$ are linearly independent over $\mathbb{Z}$ (and hence over $\mathbb{Z}[\![\Gamma]\!]$). To do this we write $b(x)$ for each $x = (x_p)_p$ in $\prod_{\mathfrak{p}\in\mathscr{P}} \mathbb{Z}$ for the smallest prime p for which $x_p \neq 0$. It is then enough to note that the inductive argument used in Lemma (3.5) (iii) can be used to construct a sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $2\cdot\Theta$ with the property that $b(x_n) < b(x_m)$ for all $n < m$.

(3.7) Remark. By using exactly the same approach as above, one can also prove variants of Theorem (3.1), such as the following.

(i) Let Σ be a finite set of rational primes and $\mathbb{Z}_\Sigma$ the subring of $\mathbb{Q}$ generated by inverting primes in Σ. Recall the group $\mathcal{E}_{\mathbb{Z}_\Sigma}$ of $\mathbb{Z}_\Sigma$-valued Euler systems (from Definition (2.1) (i)) and write $\mathcal{T}_\Sigma$ and $\mathcal{C}_\Sigma$ for the $\mathbb{Z}_\Sigma[\![\Gamma]\!]$-submodules of $\mathcal{E}_{\mathbb{Z}_\Sigma}$ generated by (the images of) $\mathcal{T}$ and $\mathcal{C}$. Then one can prove an exact analogue of Theorem (3.1) in which the roles of $\mathbb{Z}[\![\Gamma]\!], \mathcal{E}, \mathcal{T}$ and $\mathcal{C}$ are replaced by $\mathbb{Z}_\Sigma[\![\Gamma]\!], \mathcal{E}_\Sigma, \mathcal{T}_\Sigma$ and $\mathcal{C}_\Sigma$.

(ii) Write $\mathcal{E}^+$ for the $\mathbb{Z}[\![\Gamma^+]\!]$-module comprising systems $(u_E)_E$ in $\prod_{E\in\Omega^\circ_+} E^\times$ that satisfy the distributions relations (1) for all $K \subset L$ and are also such that every element u_E is totally positive. Then one can define a natural analogue $\mathrm{Ord}^+_{\mathbb{Q}}\colon \mathcal{E}^+ \to \Theta$ of the map $\mathrm{Ord}_{\mathbb{Q}}$ and the above construction shows that $\mathrm{Ord}^+_{\mathbb{Q}}$ is surjective.

4 Selmer groups for $\mathbb{G}_m$ and the proof of Theorem (1.3)

In this section we use results in § 3 to prove Theorem (1.3) and then derive several concrete observations about the Galois structure of Selmer groups of $\mathbb{G}_m$ over real abelian fields.

4.1 Preliminary observations

Fix a number field K and a set of places Σ of $\mathbb{Q}$ that contains the archimedean place ∞. The 'Σ-relative integral dual Selmer group' $\mathcal{S}_{\Sigma,\varnothing}(\mathbb{G}_{m/K})$ of $\mathbb{G}_m$ over K is the cokernel of the map

$$\prod_{w\notin\Sigma_K} \mathbb{Z} \to \mathrm{Hom}_{\mathbb{Z}}(K^\times, \mathbb{Z}), \quad (x_w)_w \mapsto \big\{a \mapsto \sum_{w\notin\Sigma_K} \mathrm{ord}_w(a)x_w\big\}.$$

This group was introduced in [BKS16, § 2.1] as an analogue for $\mathbb{G}_m$ of the integral Selmer groups of abelian varieties defined by Mazur and Tate in [MT87] and lies in an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Cl}(\mathcal{O}_{K,\Sigma}), \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathcal{S}_{\Sigma,\varnothing}(\mathbb{G}_{m/K}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathcal{O}_{K,\Sigma}^{\times}, \mathbb{Z}) \longrightarrow 0 \tag{22}$$

(cf. [BKS16, Prop. 2.2]). In the sequel we set

$$\mathcal{S}_K^{\Sigma} \coloneqq \mathcal{S}_{\Sigma,\varnothing}(\mathbb{G}_{m/K})^{\#},$$

where the superscript '#' indicates Γ_K acts on $\mathcal{S}_{\Sigma,\varnothing}(\mathbb{G}_{m/K})$ via composition with the involution of Γ_K that inverts elements. We will also write $\mathcal{S}_K$ in place of $\mathcal{S}_K^{\{\infty\}}$.

(4.1) Lemma. *Fix K and L in Ω_+ with $K \subseteq L$ and a set of places Σ as above. Then there exists a canonical map of $\mathbb{Z}[\Gamma_K]$-modules $\theta_{L/K}^{\Sigma}\colon \mathbb{Z}[\Gamma_K] \otimes_{\mathbb{Z}[\Gamma_L]} \mathcal{S}_L^{\Sigma} \to \mathcal{S}_K^{\Sigma}$. The cokernel of $\theta_{L/K}^{\Sigma}$ is finite of 2-power order and its kernel lies in an exact sequence of $\mathbb{Z}[\Gamma_K]$-modules*

$$0 \to M_{L/K,1} \to \ker(\theta_{L/K}^{\Sigma}) \to \bigoplus_{\ell \in \mathscr{P}\setminus\Sigma} \mathbb{Z}[\Gamma_K] \otimes_{\mathbb{Z}[\Gamma_{K,\ell}]} \left(\mathbb{Z}/_{n_{\ell,L/K}}\right) \to M_{L/K,2} \to 0$$

in which $M_{L/K,1}$ and $M_{L/K,2}$ are finite modules of 2-power order, $\Gamma_{K,\ell}$ is the decomposition subgroup of ℓ in Γ_K and $n_{\ell,L/K}$ the ramification degree in L/K of any (and therefore every) ℓ-adic place of K.

Proof. For L in Ω_+ we write $\Sigma(L)$ for the union of Σ and the set of places that ramify in L and for each finite set of places Σ' of $\mathbb{Q}$ containing $\Sigma(L)$ we use the complex $R\Gamma_c((\mathcal{O}_{L,\Sigma'})_{\mathcal{W}}, \mathbb{Z})$ of Γ_L-modules constructed in [BKS16, Prop. 2.4]. In particular, the latter result implies that the associated complex of R_L-modules

$$C_L^{\Sigma'} \coloneqq R\Gamma_c((\mathcal{O}_{L,\Sigma'})_{\mathcal{W}}, \mathbb{Z})^{\#}$$

is acyclic in degrees greater than three and such that

$$H^2(C_L^{\Sigma'}) = \mathcal{S}_L^{\Sigma'} \quad \text{and} \quad H^3(C_L^{\Sigma'}) = \mathrm{Hom}_{\mathbb{Z}}((L^{\times})_{\mathrm{tor}}, \mathbb{Q}/\mathbb{Z})^{\#} = \{\pm 1\}.$$

Further, since Σ' contains all places that ramify in L, the complex $C_L^{\Sigma'}$ is perfect over R_L and there is a canonical isomorphism $R_K \otimes_{R_L}^{\mathbb{L}} C_L^{\Sigma'} \cong C_K^{\Sigma'}$ in the derived category of R_K-modules. The associated Hochschield-Serre spectral sequence therefore gives rise to a homomorphism $\theta_{L/K}^{\Sigma'}\colon \mathbb{Z}[\Gamma_K] \otimes_{\mathbb{Z}[\Gamma_L]} \mathcal{S}_L^{\Sigma'} \to \mathcal{S}_K^{\Sigma'}$ whose kernel and cokernel are both finite and of 2-power order. The map $\theta_{L/K}^{\Sigma(L)}$ then induces an exact commutative diagram of R_K-modules

$$\begin{tikzcd}
 & R_K \otimes_{R_L} \Big(\prod_{w \in (\Sigma(L)\setminus\Sigma)_L} \mathbb{Z}\Big) \arrow[r, "\kappa_L"] \arrow[d, "\theta"] & R_K \otimes_{R_L} \mathcal{S}_L^{\Sigma(L)} \arrow[r] \arrow[d, "\theta_{L/K}^{\Sigma(L)}"] & R_K \otimes_{R_L} \mathcal{S}_L^{\Sigma} \arrow[r] \arrow[d, "\theta_{L/K}^{\Sigma}"] & 0 \\
0 \arrow[r] & \prod_{v \in (\Sigma(L)\setminus\Sigma)_K} \mathbb{Z} \arrow[r, "\kappa_K"] & \mathcal{S}_K^{\Sigma(L)} \arrow[r] & \mathcal{S}_K^{\Sigma} \arrow[r] & 0.
\end{tikzcd}$$

Here, for $E \in \{L, K\}$, the map κ_E is induced by the composite

$$\prod_{w \in (\Sigma(L)\setminus\Sigma)_E} \mathbb{Z}' \xrightarrow{(x_w)_w \mapsto \left\{a \mapsto \sum_{w \in (\Sigma(L)\setminus\Sigma)_E} \mathrm{ord}_w(a) x_w\right\}} \mathrm{Hom}_{\mathbb{Z}}(E^{\times}, \mathbb{Z}) \to \mathcal{S}_E^{\Sigma(L)},$$

where the second arrow is the tautological projection, and the exactness of the respective rows follows from the long exact sequence of cohomology of the exact triangle in [BKS16, Prop. 2.4 (ii)] with S, S' and T taken to be $\Sigma, \Sigma(E)$ and $\varnothing$. Further, the map θ is induced by sending each element $(n_w)_w$ of $\prod_{w \in (\Sigma(L)\setminus\Sigma)_L} \mathbb{Z}$ to $(\sum_{w|v} n_w n_{v,L/K})_v$, with $n_{v,L/K}$ the ramification degree of v in L/K. This definition ensures that the first square commutes and so $\theta_{L/K}^{\Sigma(L)}$

induces a well-defined map from $R_K \otimes_{R_L} \mathcal{S}_L^\Sigma$ to $\mathcal{S}_K^\Sigma$ that we denote by $\theta_{L/K}^\Sigma$. In particular, since the cokernel of θ is isomorphic as an R_K-module to the direct sum

$$\bigoplus_{\ell \in \mathscr{P}\setminus\Sigma} R_K \otimes_{\mathbb{Z}[\Gamma_{K,\ell}]} \left(\mathbb{Z}_{/n_{\ell,L/K}}\right),$$

the stated facts about $\ker(\theta_{L/K}^\Sigma)$ and $\mathrm{cok}(\theta_{L/K}^\Sigma)$ can be derived by applying the Snake Lemma to the above commutative diagram. □

In the case $\Sigma = \{\infty\}$, the next result verifies the first displayed equality in Theorem (1.3). We refer to a subset $\mathscr{X}$ of Ω_+ as 'cofinal' if it contains an extension of every field in Ω_+ and in any such case identify $\mathbb{Q}[\![\Gamma^+]\!]$ with $\varprojlim_{E\in\mathscr{X}} \mathbb{Q}[\Gamma_E]$ in the obvious way.

(4.2) Proposition. *For any set Σ as above, and any cofinal subset $\mathscr{X}$ of Ω_+, one has*

$$\Big(\prod_{K\in\mathscr{X}} \mathrm{Fitt}^1_{\mathbb{Z}[\Gamma_K]}(\mathcal{S}(\mathbb{G}_{m/K}))\Big) \cap \mathbb{Q}[\![\Gamma^+]\!] = 0.$$

Proof. We set $\mathbb{Z}' := \mathbb{Z}[1/2]$ and regard Σ as fixed and, for each K in Ω^+, set $\mathcal{S}'_L := \mathbb{Z}' \otimes_{\mathbb{Z}} \mathcal{S}_L^\Sigma$ and $R'_K = \mathbb{Z}'[\Gamma_K]$. Then, for every K and L in Ω_+° with $K \subseteq L$, one has

$$\pi_{L/K,\mathbb{Z}'}\big(\mathrm{Fit}^1_{R'_L}(\mathcal{S}'_L)\big) = \mathrm{Fit}^1_{R'_K}(R'_K \otimes_{R'_L} \mathcal{S}'_L) \subseteq \mathrm{Fit}^1_{R'_K}(\mathcal{S}'_K),$$

where the equality follows from a standard descent property of Fitting ideals and the inclusion from the fact that Lemma (4.1) implies that the map $\mathbb{Z}' \otimes_{\mathbb{Z}} \theta_{L/K}^\Sigma$ is surjective.

To prove the claimed result it is therefore enough to show that, for each field K in Ω_+ for which $m(K)$ is not a prime power and each natural number n, there exists an odd prime ℓ and a field L in Ω_+ that contains K and is such that

$$\pi_{L/K,\mathbb{Z}'}\big(\mathrm{Fitt}^1_{R'_L}(\mathcal{S}'_L)\big) \subseteq \ell^n \cdot \mathrm{Fitt}^1_{R'_K}(\mathcal{S}'_K).$$

To do this we fix K and n and then choose an odd prime ℓ that splits completely in K, is coprime to the order of Γ_K and does not belong to Σ. We write E_n for the unique cyclic extension of $\mathbb{Q}$ that has degree ℓ^n and is ramified only at ℓ, and L for the compositum of K and E_n. Then the field L belongs to Ω_+ and is such that a place v of K ramifies in L if and only if it is ℓ-adic, in which case its ramification degree is equal to the degree ℓ^n of L/K. In this case, therefore, Lemma (4.1) implies the existence of an exact sequence of R'_K-modules of the form

$$0 \longrightarrow R'_K/(\ell^n) \longrightarrow R'_K \otimes_{R'_L} \mathcal{S}'_L \longrightarrow \mathcal{S}'_K \longrightarrow 0. \tag{23}$$

In particular, since $\mathrm{Fit}^0_{R'_K}\big(R'_K/(\ell^n)\big) = \ell^n \cdot R'_K$, it suffices to show that (23) implies the second equality in the display

$$\pi_{L/K,\mathbb{Z}'}\big(\mathrm{Fitt}^1_{R'_L}(\mathcal{S}'_L)\big) = \mathrm{Fit}^1_{R'_K}\big(R'_K \otimes_{R'_L} \mathcal{S}'_L\big) = \mathrm{Fit}^0_{R'_K}\big(R'_K/(\ell^n)\big) \cdot \mathrm{Fit}^1_{R'_K}\big(\mathcal{S}'_K\big).$$

It is then enough to verify this after localising at each odd prime p. If $p \neq \ell$, then the localised equality is obvious since $\mathrm{Fit}^0_{R_{K,p}}(0) = R_{K,p}$. If $p = \ell$, it follows easily from the fact that $R'_{K,\ell}$ is a finite direct product of discrete valuation rings (since ℓ is prime to the order of Γ_K) and the $R'_{K,\ell}$-module $\mathcal{S}'_{K,\ell}$ has a direct summand that is free of rank one as a consequence of the exact sequence (22) and the assumption $m(K)$ is not a prime power (cf. also [Gre04, Prop. 2.2.3]). □

4.2 Euler systems, Fitting ideals, and completion of the proof of Theorem (1.3)

The next result provides a concrete link between the Selmer groups $\mathcal{S}_K$ defined in § 4.1 and the theory of Euler systems developed in earlier sections and is key to our deduction from Theorem (1.2) of the final assertion of Theorem (1.3) regarding dense subsets of Ω_+.

We write $\mathcal{I}$ for the ideal of $\mathbb{Z}[\![\Gamma^+]\!]$ given by the kernel of the natural map $\mathbb{Z}[\![\Gamma^+]\!] \to \mathbb{Z}/2\mathbb{Z}$.

(4.3) Proposition. *The map*

$$\mathbb{Q}[\![\Gamma^+]\!] \to \prod_{K\in\Omega^\circ} (\mathbb{Q}\otimes_{\mathbb{Z}} U_K), \quad q \mapsto (q_K \cdot T_\tau(c_K))_K$$

is injective. For each dense subset $\mathcal{X}$ of Ω_+ and each element $z = (z_K)_{K\in\Omega_+^\circ}$ of $\mathcal{I}^2$, this map induces a map of $\mathbb{Z}[\![\Gamma^+]\!]$-modules

$$\big(\prod_{K\in\mathcal{X}} \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K)^{-1}\big) \cap \mathbb{Q}[\![\Gamma^+]\!] \to \mathcal{E}, \quad q \mapsto (\tfrac{1}{2}z_{L^+}q_{L^+}\cdot T_\tau(c_L))_{L\in\Omega^\circ}.$$

For any system u in the image of this map one has $\mathrm{Ord}_{\mathbb{Q}}(u) \in \varpi(\mathbb{Z})$.

Proof. Fix an element $q = (q_K)_{K\in\Omega_+^\circ}$ of $\mathbb{Q}[\![\Gamma^+]\!]$. Then the image $q_{\mathbb{Q}}\cdot\mathrm{Ord}_p(c)$ of $q(T_\tau(c))$ under Ord_p is independent of p since $\mathrm{Ord}_p(c)$ is. In addition, by using the fact that $m(\mathbb{Q}(n)) = m(\mathbb{Q}(n)^+)$ for each $n > 1$ with $\mathbb{Q}(n)^+ \neq \mathbb{Q}$, one checks readily that $q(T_\tau(c))$ satisfies the distribution relations (1) since c does.
We next claim that

$$q = 0 \text{ if } q_K(c_K) = 0 \text{ for all } K \in \Omega_+^\circ. \tag{24}$$

To show this it is enough to prove the given hypotheses imply that, for each $K \in \Omega_+^\circ$ and $\chi \in \Gamma_K^*$, one has $e_\chi q_K = 0$. In addition, for each such χ, one has $e_\chi q_K = e_\chi q_{K_\chi}$ with K_χ the fixed field of $\ker(\chi)$ in K. If $\chi \neq \mathbf{1}_K$, then $K_\chi \in \Omega_+^\circ$ whilst Proposition (2.4) (i) implies $e_\chi(c_{K_\chi}) \neq 0$ and so the assumed vanishing of $q_{K_\chi}(c_{K_\chi})$ implies $e_\chi q_{K_\chi} = e_\chi q_K$ vanishes, as required. If $\chi = \mathbf{1}_K$, then $e_\chi q_K = e_\chi q_{\mathbb{Q}}$ and so it suffices to show that $q_{\mathbb{Q}}$ vanishes. But, if ℓ is any prime greater than 3, then $\mathbb{Q}(\ell)^+$ belongs to Ω_+° and so Proposition (2.4) (i) combines with the assumed vanishing of $q_{\mathbb{Q}(\ell)^+}(c_{\mathbb{Q}(\ell)^+})$ to imply that $q_{\mathbb{Q}(\ell)^+}$, and hence also $q_{\mathbb{Q}}$, vanishes, as required to complete the proof of (24).
To prove the claimed result, we now assume $q_L \in \mathrm{Fitt}^1_{R_L}(\mathcal{S}_L)^{-1}$ for all L in $\mathcal{X}$. In this case we must show that, for all elements x and y of $\mathcal{I}$ and every K in Ω_+°, the action of $\frac{1}{2}x_K y_K q_K$ on c_K gives a well-defined element of U_K. Since the kernel of the natural map $U_K \to \mathbb{Q}\otimes_{\mathbb{Z}} U_K$ is equal to $(U_K)_{\mathrm{tor}} = \{\pm 1\}$ and hence annihilated by x_K, it is thus enough to show that the element $(\frac{1}{2}y_K q_K)(c_K)$ of $\mathbb{Q}\otimes_{\mathbb{Z}} U_K$ belongs to the image $\overline{U_K}$ of U_K. Now, for every K in Ω_+° we can fix a field L in $\mathcal{X}$ such that $K \subseteq L$ and $m(L)$ and $m(K)$ have the same prime divisors. Then $\pi_{L/K,\mathbb{Q}}(y_L q_L) = y_K q_K$ and, since c satisfies (1) also $c_K = \mathrm{N}_{L/K}(c_L)$, and so

$$(y_K q_K)(c_K) = (y_K q_K)(\mathrm{N}_{L/K}(c_L)) = \mathrm{N}_{L/K}((y_L q_L)(c_L)) \in \mathbb{Q}\otimes_{\mathbb{Z}} U_K.$$

This fact allows us to assume that K belongs to $\mathcal{X}$. Then, since $\overline{U_K}$ is torsion-free, it is enough to show that for all such y_K and q_K one has

$$\theta(\tfrac{1}{2}y_K q_K(c_K)) \in R_K \quad \text{for every } \theta \text{ in } \mathrm{Hom}_{R_K}(\overline{U_K}, R_K) = \mathrm{Hom}_{R_K}(U_K, R_K). \tag{25}$$

To prove this, we note that [Tat84, Ch. IV, Lem. 1.1] allows us to express y_K as a finite sum $y_K = \sum_{i=1}^t m_i(1 - \ell_i\mathrm{Frob}_{\ell_i}^{-1})$ involving suitable integers $m_1, \ldots, m_t$ and primes $\ell_1, \ldots, \ell_t$ that are unramified in K. Since $c_{K,i} := (1 - \ell_i\mathrm{Frob}_{\ell_i}^{-1})(c_K)$ belongs to the subgroup $U_{K,i}$ of U_K comprising elements a that satisfy $a \equiv 1 \bmod \ell_i$, it is then enough to prove that one has

$$\theta(\tfrac{1}{2}q_K(c_{K,i})) \in R_K \quad \text{for all } \theta \in \mathrm{Hom}_{R_K}(U_{K,i}, R_K) \text{ and all } i \in \{1, \ldots, t\}$$

in order to verify (25). To show this we write $\iota_\#$ for the $\mathbb{Z}$-linear involution of R_K that inverts elements of Γ_K and note that, with $S(K)$ denoting the union of ∞ and the set of rational primes that ramify in K, the 'transpose' Selmer group $\mathcal{S}^{\mathrm{tr}}_{S(K),\{\ell_i\}}(\mathbb{G}_{m/K})$ defined in [BKS16, Def. 2.6] is such that

$$\begin{aligned}\mathrm{Fitt}^1_{R_K}(\mathcal{S}^{\mathrm{tr}}_{S(K),\{\ell_i\}}(\mathbb{G}_{m/K})) &\subseteq \mathrm{Fitt}^1_{R_K}(\mathcal{S}^{\mathrm{tr}}_{S(K),\varnothing}(\mathbb{G}_{m/K}))\\ &= \iota_\#\big(\mathrm{Fitt}^1_{R_K}(\mathcal{S}_{S(K),\varnothing}(\mathbb{G}_{m/K}))\big)\\ &\subseteq \iota_\#\big(\mathrm{Fitt}^1_{R_K}(\mathcal{S}_{\{\infty\},\varnothing}(\mathbb{G}_{m/K}))\big)\\ &= \mathrm{Fitt}^1_{R_K}(\mathcal{S}_{\{\infty\},\varnothing}(\mathbb{G}_{m/K})^\#)\\ &= \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K).\end{aligned}$$

Here the respective inclusions are valid since the results of [BKS16, Prop. 2.4 (i), (ii), (iii)] combine to imply the existence of surjective maps of R_K-modules from $\mathcal{S}^{\mathrm{tr}}_{S(K),\{\ell_i\}}(\mathbb{G}_{m/K})$ to $\mathcal{S}^{\mathrm{tr}}_{S(K),\varnothing}(\mathbb{G}_{m/K})$ and from $\mathcal{S}_{S(K),\varnothing}(\mathbb{G}_{m/K})$ to $\mathcal{S}_{\{\infty\},\varnothing}(\mathbb{G}_{m/K})$. In addition, the first equality follows from [BKS16, Lem. 2.8], the second equality is clear and the third equality follows from our definition of the module $\mathcal{S}_K$.

The key point now is that, for every $\theta \in \mathrm{Hom}_{R_K}(U_{K,i}, R_K)$, the first assertion of [BKS16, Th. 7.5] implies $\theta(\frac{1}{2}c_{K,i})$ belongs to $\mathrm{Fitt}^1_{R_K}(\mathcal{S}^{\mathrm{tr}}_{S(K),\{\ell_i\}}(\mathbb{G}_{m/K}))$ and hence, since $K \in \mathcal{X}$, that

$$\begin{aligned}\theta(\tfrac{1}{2}q_K(c_{K,i})) = q_K \cdot \theta(\tfrac{1}{2}c_{K,i}) &\in \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K)^{-1} \cdot \mathrm{Fitt}^1_{R_K}(\mathcal{S}^{\mathrm{tr}}_{S(K),\{\ell_i\}}(\mathbb{G}_{m/K}))\\ &\subseteq \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K)^{-1} \cdot \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K)\\ &\subseteq R_K,\end{aligned}$$

as required. □

To complete the proof of Theorem (1.3), it now remains to prove the second displayed equality in said result. For this purpose it is enough to fix a dense subset $\mathcal{X}$ of Ω_+ and show that every element q of the intersection $\big(\prod_{K\in\mathcal{X}} \mathrm{Fitt}^1_{R_K}(\mathcal{S}_K)^{-1}\big) \cap \mathbb{Q}[\![\Gamma^+]\!]$ belongs to $\mathbb{Z}[\![\Gamma^+]\!]$.

Now, upon fixing an arbitrary element z of $\mathcal{I}^2$, any such q gives rise, via Proposition (4.3), to a system $u_{z,q} := (\frac{1}{2}zqT_\tau)(c)$ in $\mathcal{E}$. In addition, the system $zq\cdot T_\tau(c) = T_\tau(u_{z,q})$ belongs to $T_\tau(\mathcal{E})$ and is sent by $\mathrm{Ord}_{\mathbb{Q}}$ to an element of $\varpi(\mathbb{Z})$. From the injectivity of the second map in (21) we can therefore deduce the existence of an element r of $\mathbb{Z}[\![\Gamma^+]\!]$ for which one has

$$(zqT_\tau)(c) = T_\tau(u_{z,q}) = r(T_\tau(c)) \in T_\tau(\mathcal{E}).$$

Given the injectivity of the map in Proposition (4.3), this implies that $zq = r$ belongs to $\mathbb{Z}[\![\Gamma^+]\!]$, and hence that $q\cdot(\mathcal{I})^2 \subseteq \mathbb{Z}[\![\Gamma^+]\!]$. To complete the proof of Theorem (1.3), it is therefore enough to prove (and then apply twice) the equality

$$\{v \in \mathbb{Q}[\![\Gamma^+]\!] \mid v\cdot\mathcal{I} \subseteq \mathbb{Z}[\![\Gamma^+]\!]\} = \mathbb{Z}[\![\Gamma^+]\!].$$

To do this, we take an element $v = (v_K)_K$ and note that, for each $K \in \Omega_+^\circ$, one has $v_K\cdot\mathcal{I}_K \subseteq R_K$ with $\mathcal{I}_K := \ker\{R_K \to \mathbb{Z}/2\mathbb{Z}\}$. Now, a direct computation shows that $\{a \in R_K \mid a\cdot\mathcal{I}_K \subseteq R_K\}$ is equal to $\frac{1}{2}\mathbb{Z}\cdot T_K + R_K$, and so we may write $v_K = \frac{1}{2}n_KT_K + r_K$ for suitable $n_K \in \mathbb{Z}$ and $r_K \in R_K$. Given an arbitrary field $K \in \Omega_+^\circ$, we can then choose a quadratic extension $L \in \Omega_+^\circ$ of K and deduce that the element

$$v_K = \pi_{L/K}(v_L) = \pi_{L/K}(\tfrac{1}{2}n_LT_L + r_L) = \pi_{L/K}(n_L)T_K + \pi_{L/K}(r_L)$$

belongs to R_K, as required. □

(4.4) Remark. Just as in Remark (3.7) (i), the above approach can be used to prove 'localized' versions of Theorem (1.3) in which $\mathbb{Z}$ is replaced by $\mathbb{Z}_\Sigma$ for a finite set of rational primes Σ.

4.3 Galois structures of Selmer groups

For any odd prime ℓ, there are infinitely many fields K in Ω_+ for which ℓ divides both $[K:\mathbb{Q}]$ and $|\mathrm{Cl}(\mathcal{O}_K)|$ (cf. Cornell and Washington [CW85, § 2, Cor.]). This suggests that, as K ranges over Ω_+, the structure of the Γ_K-module $\mathrm{Cl}(\mathcal{O}_K)$ can be complicated and, as far as we are aware, there are no general structural results about the class groups of real abelian fields.

Nevertheless, it is straightforward to deduce concrete information about the Galois structures of Selmer groups from Theorem (1.3), as in the following result. In claim (ii) of this result we set $\mathbb{Z}' := \mathbb{Z}[1/2]$ and $M' := \mathbb{Z}' \otimes_{\mathbb{Z}} M$ for each Γ_E-module M.

(4.5) Corollary. *Fix a non-zero ideal I of $\mathbb{Z}[\![\Gamma^+]\!]$ and for K in Ω_+ write I_K for its image in $\mathbb{Z}[\Gamma_K]$. Let $\mathcal{X}$ be a cofinal subset of Ω_+ and for each K in Ω_+ write $\mathcal{X}_K$ for the subset of $\mathcal{X}$ comprising extensions of K. Then the following claims are valid.*

(i) For every K in Ω_+ there exist infinitely many E in $\mathcal{X}_K$ for which at least one of the $\mathbb{Z}[\Gamma_E]$-modules $I_E \cdot \mathcal{S}_E$ and $\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)$ is not cyclic.

(ii) Assume $I^{-1} := \{\lambda \in \mathbb{Q}[\![\Gamma^+]\!] : \lambda I \subseteq \mathbb{Z}'[\![\Gamma^+]\!]\}$ is not equal to $\mathbb{Z}'[\![\Gamma^+]\!]$. Assume also that for all fields K in some dense subset of Ω_+ the set $\mathcal{X}_K$ contains fields whose degrees over K are coprime. Then there are infinitely many E in $\mathcal{X}$ for which the $\mathbb{Z}'[\Gamma_E]/I'_E$-module $\mathcal{S}'_E/(I'_E \cdot \mathcal{S}'_E)$ has no quotient that is free of rank two.

Proof. By a standard property of Fitting ideals (cf. [Nor76, § 3.1, Exer. 2]), the tautological exact sequence $0 \to I_E \cdot \mathcal{S}_E \to \mathcal{S}_E \to \mathcal{S}_E/(I_E \cdot \mathcal{S}_E) \to 0$ implies an inclusion

$$\mathrm{Fitt}^1_{R_E}(I_E \cdot \mathcal{S}_E) \cdot \mathrm{Fitt}^0_{R_E}\big(\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)\big) \subseteq \mathrm{Fitt}^1_{R_E}(\mathcal{S}_E).$$

In addition, if $I_E \cdot \mathcal{S}_E$ and $\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)$ are cyclic R_E-modules, then $\mathrm{Fitt}^1_{R_E}(I_E \cdot \mathcal{S}_E) = R_E$ and $\mathrm{Fitt}^0_{R_E}\big(\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)\big)$ is equal to the annihilator of $\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)$ in R_E and so contains I_E. In any such case therefore, the above inclusion implies that $\mathrm{Fitt}^1_{R_E}(\mathcal{S}_E)$ contains I_E.

To prove claim (i) it is enough to show each set $\mathcal{X}_K$ contains at least one field E for which the R_E-modules $I_E \cdot \mathcal{S}_E$ and $\mathcal{S}_E/(I_E \cdot \mathcal{S}_E)$ are not both cyclic. To do this we argue by contradiction and so assume $K \in \Omega_+$ is such that, for every E in $\mathcal{X}_K$, the R_E-modules $I \cdot \mathcal{S}_E$ and $\mathcal{S}_E/(I \cdot \mathcal{S}_E)$ are cyclic. Then, as $\mathcal{X}_K$ is cofinal in Ω_+, the above observations imply inclusions

$$(0) \neq I \subseteq \varprojlim_{E \in \Omega_+} I_E = \varprojlim_{E \in \mathcal{X}_K} I_E \subseteq \big(\prod_{E \in \mathcal{X}_K} \mathrm{Fitt}^1_{R_E}(\mathcal{S}_E)\big) \cap \mathbb{Q}[\![\Gamma^+]\!]$$

and these inclusions contradict the result of Proposition (4.2).

To prove claim (ii) we set $R'_E := \mathbb{Z}'[\Gamma_E]$ and again argue by contradiction. We therefore assume, after shrinking $\mathcal{X}$ if necessary, that for every E in $\mathcal{X}$ the R'_E/I'_E-module $\mathcal{S}'_E/(I'_E \cdot \mathcal{S}'_E)$ has a free quotient of rank two. In this case, for every such E, the ideal $\mathrm{Fitt}^1_{R'_E/I'_E}\big(\mathcal{S}'_E/(I'_E \cdot \mathcal{S}'_E)\big)$ vanishes and so $\mathrm{Fitt}^1_{R'_E}(\mathcal{S}'_E) \subseteq I'_E$. One therefore has a chain of inclusions

$$\mathbb{Z}'[\![\Gamma^+]\!] \subsetneq I^{-1} \subseteq \big(\prod_{E \in \mathcal{X}} \mathrm{Fitt}^1_{R'_E}(\mathcal{S}'_E)^{-1}\big) \cap \mathbb{Q}[\![\Gamma^+]\!],$$

in which the first is, by assumption, strict. We now fix a dense subset $\mathcal{X}'$ of Ω_+ with the stated property. Then it is enough to show that

$$\big(\prod_{E \in \mathcal{X}} \mathrm{Fitt}^1_{R'_E}(\mathcal{S}'_E)^{-1}\big) \cap \mathbb{Q}[\![\Gamma^+]\!] \subseteq \big(\prod_{E \in \mathcal{X}'} \mathrm{Fitt}^1_{R'_E}(\mathcal{S}'_E)^{-1}\big) \cap \mathbb{Q}[\![\Gamma^+]\!],$$

since this would imply that the above inclusions contradict the second displayed equality in Theorem (1.3) with $\mathcal{X}$ replaced by $\mathcal{X}'$ (and taking account of Remark (4.4) (ii)). To prove this it suffices to fix $q = (q_E)_{E \in \Omega_+}$ in $\mathbb{Q}[\![\Gamma^+]\!]$ with $q_E \in \mathrm{Fitt}^1_{R'_E}(\mathcal{S}'_E)^{-1}$ for all $E \in \mathcal{X}$ and show that q_K belongs to $\mathrm{Fitt}^1_{R'_K}(\mathcal{S}'_K)^{-1}$ for every $K \in \mathcal{X}'$.

To do this we fix K in $\mathcal{X}'$ and fields K_1 and K_2 in $\mathcal{X}_K$ of coprime degrees over K. Then, for $i \in \{1, 2\}$, Lemma (4.1) implies that $\pi_{K_i/K,\mathbb{Z}'}(\mathrm{Fitt}^1_{R'_{K_i}}(\mathcal{S}_{K_i}))$ is a submodule of $\mathrm{Fitt}^1_{R'_K}(\mathcal{S}'_K)$ whose index is finite and divides a power of $d_i := [K_i : K]$. For any sufficiently large integer m one therefore has

$$d_i^m \cdot q_K = d_i^m \cdot \pi_{K_i/K,\mathbb{Q}}(q_{K_i}) \in d_i^m \cdot \pi_{K_i/K,\mathbb{Q}}(\mathrm{Fitt}^1_{R'_{K_i}}(\mathcal{S}'_{K_i})^{-1}) \subseteq \mathrm{Fitt}^1_{R'_K}(\mathcal{S}'_K)^{-1}$$

and, since d_1 and d_2 are coprime, this implies $q_K \in \mathrm{Fitt}^1_{R'_K}(\mathcal{S}'_K)^{-1}$, as required. □

(4.6) Remark. The conditions required to apply Corollary (4.5) (ii) are satisfied in a variety of concrete situations, such as the following.
(i) An ideal I of $\mathbb{Z}[\![\Gamma^+]\!]$ satisfies the stated condition if it is proper and invertible. In particular, this is true if I is principal with a generator in $\mathbb{Q}[\![\Gamma^+]\!]^\times \setminus \mathbb{Z}[\![\Gamma^+]\!]^\times$.
(ii) A subset $\mathcal{X}$ of Ω_+ automatically satisfies the stated condition if it is itself dense. As a concrete example, for any function $f\colon \mathbb{N} \to \mathbb{N}$ the set $\mathcal{X}_f = \{\mathbb{Q}(n^{f(n)})^+ : n \in \mathbb{N}\}$ is dense.
(iii) Assume I is the principal ideal generated by an odd prime p, fix a function f as in (ii) and for each natural number n set $E_n := \mathbb{Q}(n^{f(n)})^+$. Then the stated result implies the existence of infinitely many n for which the Γ_{E_n}-module $\mathcal{S}_{E_n}$ has no quotient isomorphic to $(\mathbb{Z}/(p))[\Gamma_{E_n}]^2$.

References

[Bul+23] Dominik Bullach, David Burns, Alexandre Daoud and Seo Soogil. *Dirichlet L-series at $s = 0$ and the scarcity of Euler systems.* 2023. arXiv: 2111.14689.

[BKS16] David Burns, Masato Kurihara and Takamichi Sano. *On zeta elements for $\mathbb{G}_m$.* Doc. Math. 21 (2016), pp. 555–626.

[BS21] David Burns and Soogil Seo. *On circular distributions and a conjecture of Coleman.* Israel J. Math. 241.1 (2021), pp. 343–393.

[Col79] Robert F. Coleman. *Division values in local fields.* Invent. Math. 53.2 (1979), pp. 91–116.

[Col85] Robert F. Coleman. *On an Archimedian characterization of the circular units.* J. Reine Angew. Math. 356 (1985), pp. 161–173.

[CW85] Gary Cornell and Lawrence C. Washington. *Class numbers of cyclotomic fields.* J. Number Theory 21.3 (1985), pp. 260–274.

[Gre04] Cornelius Greither. "Arithmetic annihilators and Stark-type conjectures". In: *Stark's conjectures: recent work and new directions.* Vol. 358. Contemp. Math. Amer. Math. Soc., Providence, RI, 2004, pp. 55–78.

[KL81] Daniel S. Kubert and Serge Lang. *Modular units.* Vol. 244. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York-Berlin, 1981, pp. xiii+358.

[MR04] Barry Mazur and Karl Rubin. *Kolyvagin systems.* Mem. Amer. Math. Soc. 168.799 (2004), pp. viii+96.

[MT87] Barry Mazur and John Tate. *Refined Conjectures of the Birch and Swinnerton-Dyer Type.* Duke Math. J. 54 (1987), pp. 711–750.

[NSW08] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg. *Cohomology of number fields.* Second. Vol. 323. Fundamental Principles of Mathematical Sciences. Springer-Verlag, Berlin, 2008.

[Nor76] D. G. Northcott. *Finite free resolutions.* Cambridge Tracts in Mathematics, No. 71. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[Rub00] Karl Rubin. *Euler systems.* 147. Princeton University Press, 2000.

[Seo01] Soogil Seo. *Circular distributions and Euler systems.* J. Number Theory 88.2 (2001), pp. 366–379.

[Seo04] Soogil Seo. *A note on circular distributions.* Acta Arith. 114.4 (2004), pp. 313–322.

[Seo06] Soogil Seo. *Circular distributions of finite order.* Math. Res. Lett. 13.1 (2006), pp. 1–14.

[Seo08] Soogil Seo. *Truncated Euler systems.* J. Reine Angew. Math. 614 (2008), pp. 53–71.

[Sin80] Warren Sinnott. *On the Stickelberger ideal and the circular units of an abelian field.* Invent. Math. 62.2 (1980), pp. 181–234.

[Tat84] John T. Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$.* Progress in Mathematics 47 (1984).

[Tha88] Francisco Thaine. *On the ideal class groups of real abelian number fields.* Ann. of Math. (2) 128.1 (1988), pp. 1–18.

King's College London, Department of Mathematics, London WC2R 2LS, UK
Email addresses: dominik.bullach@kcl.ac.uk, david.burns@kcl.ac.uk, alexandre.daoud@kcl.ac.uk

Yonsei University, Department of Mathematics, Seoul, Korea.
Email address: sgseo@yonsei.ac.kr