ON CIRCULAR DISTRIBUTIONS AND A CONJECTURE OF COLEMAN

DAVID BURNS AND SOOGIL SEO*

Abstract. We obtain strong new evidence in support of a conjecture of Robert Coleman concerning the module of circular distributions.

1. Introduction

In the Introduction to [9] Kubert and Lang describe how the general theory of distributions has a prominent role in number theory research and is strongly influenced by the classical theory of cyclotomic numbers in abelian fields. A similar point is also made by Washington in [22, Chap. 12].

This article is concerned with an important class of such distributions. To give some details we fix an algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$ and for each natural number m write μ_m for the group of m-th roots of unity in $\mathbb{Q}^c$ and set $\mu_m^* := \mu_m \setminus \{1\}$. We also write μ_∞ for the union of μ_m over all m, set $\mu_\infty^* := \mu_\infty \setminus \{1\}$ and write $\mathcal{F}$ for the multiplicative group comprising functions from μ_∞^* to $\mathbb{Q}^{c,\times}$ that respect the natural action of $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$.

Then, in the 1980s Coleman defined a 'circular distribution', or 'distribution' for short in the sequel, to be a function f in $\mathcal{F}$ that satisfies the relation

$$(1) \qquad \prod_{\zeta^a=\varepsilon} f(\zeta) = f(\varepsilon)$$

for all natural numbers a and all ε in μ_∞^*. (A similar notion was also subsequently introduced by Coates in [1] in the context of abelian extensions of imaginary quadratic fields.)

We write $\mathcal{F}^{\mathrm{d}}$ for the subgroup of $\mathcal{F}$ comprising all distributions and further define the group of 'strict distributions' to be the subgroup $\mathcal{F}^{\mathrm{sd}}$ of $\mathcal{F}^{\mathrm{d}}$ comprising distributions that satisfy the congruence relation

$$(2) \qquad f(\varepsilon\cdot\zeta) \equiv f(\zeta) \text{ modulo all primes above } \ell$$

for all natural numbers n, all primes ℓ that are coprime to n, all ε in μ_ℓ and all ζ in μ_n^*.

It is clear that each of the groups $\mathcal{F}, \mathcal{F}^{\mathrm{d}}$ and $\mathcal{F}^{\mathrm{sd}}$ is naturally a module over the ring

$$R := \varprojlim_n \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q})],$$

where we write $\mathbb{Q}(n)$ for the field $\mathbb{Q}(\mu_n)$ and the transition morphisms in the inverse limit are induced by the natural restriction maps.

[0]The second author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2019R1F1A1043646).

2000 *Mathematics Subject Classification.* Primary: 11R42; Secondary: 11R27.

As far as explicit examples are concerned, the function Φ in $\mathcal{F}$ that is defined by setting

$$\Phi(\zeta) := 1 - \zeta \quad \text{for all } \zeta \text{ in } \mu_\infty^*$$

belongs to $\mathcal{F}^{\mathrm{sd}}$. We shall write $\mathcal{F}^{\mathrm{c}}$ for the R-submodule of $\mathcal{F}^{\mathrm{sd}}$ generated by Φ and refer to elements of $\mathcal{F}^{\mathrm{c}}$ as 'cyclotomic distributions'.

In addition, Coleman observed that for any non-empty set Π of odd prime numbers the function δ_Π in $\mathcal{F}$ with

$$\delta_\Pi(\zeta) := \begin{cases} -1, & \text{if the order of } \zeta \text{ is divisible only by primes that belong to } \Pi, \\ 1, & \text{otherwise} \end{cases}$$

belongs to $\mathcal{F}^{\mathrm{d}}$ and, in addition, that the only such function belonging to $\mathcal{F}^{\mathrm{sd}}$ is $\delta_{\mathrm{odd}} := \delta_{\Pi_{\mathrm{odd}}}$ where Π_{odd} denotes the set of all odd primes. We shall write $\mathcal{D}$ for the R-submodule of $\mathcal{F}^{\mathrm{d}}$ generated by the set of all functions of the form δ_Π and refer to these functions as 'Coleman distributions'.

Then, in 1989, Coleman was led to make the following remarkable conjecture.

Conjecture 1.1 (Coleman)**.** $\mathcal{F}^{\mathrm{d}} = \mathcal{D} + \mathcal{F}^{\mathrm{c}}$.

This conjecture was motivated by the archimedean characterization of cyclotomic units that Coleman had given in [3] and is therefore related to attempts to understand a globalized 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 been proved in [2].

The second author was subsequently able to show in [17] and [18] both that $\mathcal{D}$ is equal to the full torsion subgroup of $\mathcal{F}^{\mathrm{d}}$, and hence that the torsion subgroup of $\mathcal{F}^{\mathrm{sd}}$ is generated by the single Coleman distribution δ_{odd}, and also that $\mathcal{F}^{\mathrm{c}}$ is torsion-free.

This meant, in particular, that Coleman's Conjecture was valid if and only if the inclusion $\mathcal{F}^{\mathrm{c}} \subseteq \mathcal{F}^{\mathrm{d}}$ induces an identification

$$\mathcal{F}^{\mathrm{c}} = \mathcal{F}^{\mathrm{d}}_{\mathrm{tf}} \tag{3}$$

where we write $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}$ for the quotient of $\mathcal{F}^{\mathrm{d}}$ by its torsion subgroup $\mathcal{D}$.

However, it has since proved to be very difficult to decide whether the equality (3) is valid and, until now, all existing results in this direction have in effect only considered the much weaker question of whether, for any given distribution f and any given root of unity ζ in μ_∞^* there exists an element $r_{f,\zeta}$ of R such that $f(\zeta) = \Phi(\zeta)^{r_{f,\zeta}}$? Such results include, for example, those that are obtained by the second author in [15, 16, 17] and the related results of Saikia in [14]. (For the convenience of the reader we also mention already here that some arguments in [15] and [16] require clarification and/or correction; for details see Remark 3.6.)

By contrast, we shall now develop techniques that allow a systematic investigation of the conjectural equality (3) itself.

To give an example of the sort of results that we are able to prove we write $\widehat{R}$ for the profinite completion of R. We also denote complex conjugation by τ and regard it as an element of R in the obvious way.

We write $\widehat{\mathbb{Z}}(1)$ for the inverse limit of the groups μ_m with respect to the transition morphisms $\mu_m \to \mu_{m'}$ for each divisor m' of m that are given by raising to the power m/m'. We observe that $\widehat{\mathbb{Z}}(1)$ is naturally an R-module.

Then the following result will be proved in §6.1.

Theorem 1.2. *There exists a canonical exact commutative diagram of R-modules of the form*

$$\begin{tikzcd} \widehat{\mathbb{Z}}(1) \arrow[r, hook] & \mathcal{F}^{\mathrm{d}}_{\mathrm{tf}} \arrow[r, "\kappa"] & \widehat{R}(1+\tau) \\ \widehat{\mathbb{Z}}(1) \arrow[r, hook] \arrow[u, equal] & \mathcal{F}^{\mathrm{c}} \arrow[r, two heads] \arrow[u, hook] & R(1+\tau). \arrow[u, hook] \end{tikzcd}$$

(We note that the two vertical arrows in this diagram are the natural inclusions and that all other maps will be defined explicitly in the course of the proof.)

This result is of interest for several reasons.

Firstly, for example, it reduces the study of $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}$ to the study of $(1+\tau)\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}$ and identifies this module with a submodule of the profinite completion of $(1+\tau)\mathcal{F}^{\mathrm{c}}$, thereby showing that Coleman's Conjecture is, in a natural sense, true 'everywhere locally'.

Secondly, Theorem 1.2 will allow us to establish (in Theorem 6.7) an explicit 'p-adic' criterion for a distribution to be cyclotomic that is very reminiscent of the 'archimedean boundedness' criterion used in [3] to characterise cyclotomic units (and which itself motivated Coleman's study of circular distributions).

Thirdly, our approach allows us to show that for every prime p the quotient group $Q := \mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}}$ identifies with a submodule of a canonical uniquely p-divisible group and, in addition, to give an explicit criterion for the image in Q of a distribution to be p-divisible. In fact, it seems to us possible that further development of the methods introduced here may allow one to prove that Q is itself uniquely divisible, and for all practical purposes concerning applications to the theory of Euler systems this would be enough (see the discussion in §7.2).

In the course of proving Theorem 1.2 we shall also establish several auxiliary results that are perhaps themselves of interest.

Such results include an unconditional proof of the main result of the second author in [15] that in loc. cit. is only proved modulo the validity of Greenberg's conjecture on the ideal class groups of real abelian fields (see Theorem 3.1 and Remark 3.6), a complete characterization of torsion-valued distributions (see Theorem 4.1) and a more conceptual proof of the fact that $\mathcal{D}$ is equal to the torsion subgroup of $\mathcal{F}^{\mathrm{d}}$, as discussed above (see Remark 4.5).

Finally, we note that the short exact sequence in the lower row of the diagram in Theorem 1.2 splits after inverting 2, but not otherwise.

In fact, an investigation of the submodule $\mathcal{F}^{\mathrm{d},\tau=1}$ of $\mathcal{F}^{\mathrm{d}}$ comprising distributions fixed by the action of τ plays an important role in our approach and, in particular, the difficulty of explicitly characterizing $(1+\tau)\mathcal{F}^{\mathrm{d}}$ as a submodule of $\mathcal{F}^{\mathrm{d},\tau=1}$ often causes extra complications when considering 2-primary aspects of problems (the quotient group $\mathcal{F}^{\mathrm{d},\tau=1}/(1+\tau)\mathcal{F}^{\mathrm{d}}$ is a vector space over the field of two elements of uncountably infinite dimension - see

Remark 6.3). We are able to resolve many, but not all, of these 2-primary issues and, as a consequence, some of our results are slightly less complete than we would have liked.

In a little more detail, the main contents of this article is as follows. In §2 we recall some basic facts concerning distributions, introduce various useful notions of 'partial distribution', prove several technical results concerning distributions with totally positive values that are important for later arguments and discuss various explicit examples that give some idea of the difficulties that can arise when working with distributions. In §3 we recall the well-known link between distributions and Euler systems and combine this with results of Greither to establish (in Theorem 3.1) a concrete link between the values of distributions in the groups $\mathcal{F}^{\rm d}$ and $\mathcal{F}^{\rm c}$. In this section we will also point out an error in the proof of the main result of [15] (see Remark 3.6). In §4 we make a detailed study of distributions that are valued in roots of unity and prove (in Theorem 4.1) an important reduction step in the proof of Theorem 1.2. In §5 we prove (in Theorem 5.1) several key properties of distributions 'of prime level' and then, in §6, we shall combine the results of §4 and §5 to prove Theorem 1.2 and also justify the various remarks that are made after the above statement of this result. Finally, in §7 we shall use Theorem 1.2 to give an explicit criterion for the image of a distribution in $\mathcal{F}^{\rm d}_{\rm tf}/\mathcal{F}^{\rm c}$ to be p-divisible and also show that 'divisible' distributions have many of the same properties as cyclotomic distributions.

Throughout the article we shall usually use exponential notation to indicate the action of a commutative ring Λ on a multiplicative group U, so that the image of an element u of U under the action of an element λ of Λ is written as u^λ. However we caution the reader that, for typographic simplicity, we shall also occasionally write either $\lambda(u)$ or $\lambda\cdot u$ in place of u^λ.

Acknowledgements It is a pleasure to thank the anonymous referee for a careful reading of our article and for several helpful remarks.

2. Basic properties of distributions

In this section we shall first recall some well-known properties of distributions. We next establish several further properties that will be useful in later arguments and then end by discussing various explicit examples that help clarify the theory.

2.1. We first introduce notation and review some basic facts concerning distributions (that are in the main due to Coleman).

2.1.1. In the sequel we set $\mathbb{N}^* := \mathbb{N}\setminus\{1\}$.

For each n in $\mathbb{N}^*$ we fix a generator ζ_n of μ_n such that $\zeta_{mn}^m = \zeta_n$ for all m and n and for each function f in $\mathcal{F}$ we set

$$f(n) := f(\zeta_n).$$

Having made such a choice of elements of μ_∞^*, the Galois equivariance of functions in $\mathcal{F}^{\rm d}$ allows us to identify each such f with a set of the form $\{f(n)\}_{n\in\mathbb{N}^*}$, where each $f(n)$ belongs to $\mathbb{Q}(n)^\times$ and, taken together, these elements satisfy suitable relations.

Before stating these relations we introduce some further notation. We set

$$G_n := \mathrm{Gal}(\mathbb{Q}(n)/\mathbb{Q}) \quad\text{and}\quad R_n := \mathbb{Z}[G_n].$$

For each multiple m of n we then write G_n^m for the subgroup $\mathrm{Gal}(\mathbb{Q}(m)/\mathbb{Q}(n))$ of G_m and π_n^m for the ring homomorphism $R_m \to R_n$ induced by the natural projection $G_m \to G_n$. We also write N_n^m for the field-theoretic norm map $\mathbb{Q}(m)^\times \to \mathbb{Q}(n)^\times$.

We write τ for the element of G_n induced by complex conjugation and note that the maximal totally real subfield $\mathbb{Q}(n)^+$ of $\mathbb{Q}(n)$ is equal to the set of elements fixed by τ.

For each prime ℓ we fix an element σ_ℓ of $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ that restricts to give the identify automorphism on $\mathbb{Q}(\ell^a)$ for all natural numbers a and to give the *inverse* of the Frobenius element at ℓ on $\mathbb{Q}(m)$ for every natural number m that is prime to ℓ.

Then a straightforward exercise shows that the defining property (1) of f is equivalent to requiring that for each natural number m in $\mathbb{N}^*$ and each prime ℓ one has

$$\mathrm{N}_m^{m\ell}(f(m\ell)) = \begin{cases} f(m), & \text{if } \ell \text{ divides } m,\\ f(m)^{1-\sigma_\ell}, & \text{if } \ell \text{ is prime to } m.\end{cases} \tag{4}$$

We write $E(n)$ and $E^p(n)$ for each prime p for the group of global units, respectively global p-units, in $\mathbb{Q}(n)$ and set

$$E(n)' := \begin{cases} E^p(n), & \text{if } n \text{ is a power of a prime } p,\\ E(n), & \text{otherwise.}\end{cases}$$

Then the first distribution relation in (4) implies that for each n in $\mathbb{N}^*$ one has

$$f(n) \in E(n)' \tag{5}$$

(for details see, for example, [15, Lem. 2.2]).

2.1.2. For any non-empty subset Σ of $\mathbb{N}^*$ we shall write μ_Σ^* for the $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$-invariant subset of μ_∞^* comprising all roots of unity whose (exact) order belongs to Σ.

We also write $\mathcal{F}_\Sigma^{\mathrm{d}}$ for the multiplicative group of $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$-equivariant maps from μ_Σ^* to $\mathbb{Q}^{c,\times}$ that satisfy the relation (1) for all ε in μ_Σ^* and all natural numbers a for which there exists an element ζ of μ_Σ^* such that $\zeta^a = \varepsilon$.

We then write $\mathcal{F}_\Sigma^{\mathrm{sd}}$ for the subgroup of $\mathcal{F}_\Sigma^{\mathrm{d}}$ comprising functions that also satisfy the congruence relation (2) for all coprime n and ℓ for which n and $n \cdot \ell$ both belong to Σ.

It is clear that each such group $\mathcal{F}_\Sigma^{\mathrm{d}}$ and $\mathcal{F}_\Sigma^{\mathrm{sd}}$ has a natural structure as R-module and we write ι_Σ for both of the homomorphisms of R-modules $\mathcal{F}^{\mathrm{d}} \to \mathcal{F}_\Sigma^{\mathrm{d}}$ and $\mathcal{F}^{\mathrm{sd}} \to \mathcal{F}_\Sigma^{\mathrm{sd}}$ that are obtained by restricting functions from μ_∞^* to μ_Σ^*.

In the special case that Σ is equal to the subset $\mathbb{N}(m)$ of $\mathbb{N}^*$ comprising all multiples of a given natural number m with $m > 1$, then we shall abbreviate $\mathcal{F}_\Sigma^{\mathrm{d}}$ and $\mathcal{F}_\Sigma^{\mathrm{sd}}$ to $\mathcal{F}_{(m)}^{\mathrm{d}}$ and $\mathcal{F}_{(m)}^{\mathrm{sd}}$ and refer to functions in these sets as 'distributions of level m' and 'strict distributions of level m' respectively. In this case we shall also write ι_m in place of ι_Σ.

2.2. In this section we establish several useful results concerning distributions with totally positive values.

For each m in $\mathbb{N}^*$ we write $\mathbb{Q}(m)^+_{>0}$ for the multiplicative group of totally positive elements in $\mathbb{Q}(m)^+$ and then define a torsion-free group by setting

$$V(m) := E(m)' \cap \mathbb{Q}(m)^+_{>0}.$$

For each subset Σ of $\mathbb{N}^*$ we write $\mathcal{F}_\Sigma^{\mathrm{d},+}$ and $\mathcal{F}_\Sigma^{\mathrm{sd},+}$ for the R-submodules of $\mathcal{F}_\Sigma^{\mathrm{d}}$ and $\mathcal{F}_\Sigma^{\mathrm{sd}}$ comprising functions f with $f(m) \in V(m)$ for all m in Σ.

Lemma 2.1. *If Σ is any cofinal subset of $\mathbb{N}^*$ that is closed under taking powers, then the natural restriction map $\iota_\Sigma : \mathcal{F}^{\mathrm{d},+} \to \mathcal{F}_\Sigma^{\mathrm{d},+}$ is injective.*

Proof. To argue by contradiction we assume f is a non-trivial distribution with $\iota_\Sigma(f) = 1$. We fix m in $\mathbb{N}^*$ with $f(m) \neq 1$ and a prime divisor p of m. We then fix a natural number n in $\Sigma \cap \mathbb{N}(m)$ and note that, since Σ is closed under taking powers, for each $a \in \mathbb{N}$ there exists a natural number n_a in $\Sigma \cap \mathbb{N}(mp^a)$ that has the same prime divisors as n.

In particular, if we write $\mathcal{P}$ for the (possibly empty) set of primes that divide n but not m, and hence divide n_a but not mp^a, then for each a one has

$$1 = \mathrm{N}_{mp^a}^{n_a}(1) = \mathrm{N}_{mp^a}^{n_a}(f(n_a)) = f(mp^a)^{\prod_\ell (1-\sigma_\ell)}$$

where in the product ℓ runs over all primes in $\mathcal{P}$.

If $\mathcal{P}$ is empty, this implies $f(mp^a) = 1$ and hence also, since p divides m, that $f(m) = \mathrm{N}_m^{mp}(f(mp)) = 1$, which is a contradiction.

On the other hand, if $\mathcal{P}$ is non-empty, then, since the elements $f(mp^a)$ for $a \geq 0$ form a norm-compatible family of elements of $V(mp^a)$, we obtain a contradiction to the assumption $f(m) \neq 1$ by successively applying Lemma 2.2 below with q taken to be each of the primes in $\mathcal{P}$. □

Lemma 2.2. *Fix m in $\mathbb{N}^*$ and a prime divisor p of m. Let $(x_a)_{a \geq 0}$ be a norm compatible family of elements of $V(mp^a)$ for which there exists a prime q that does not divide m and is such that $x_a^{1-\sigma_q} = 1$ for all a. Then one has $x_0 = 1$.*

Proof. Since the image of σ_q in $\mathrm{Gal}(\mathbb{Q}(mp^\infty)/\mathbb{Q})$ generates an open subgroup, each element x_a belongs to $\mathbb{Q}(mp^d)$ for a fixed natural number d.

Thus, for each integer $e > d$ one has

$$x_0 = \mathrm{N}_m^{mp^e}(x_e) = \mathrm{N}_m^{mp^d}(x_e)^{p^{e-d}} \in V(m)^{p^{e-d}}.$$

Given this, the triviality of x_0 follows from the fact that the intersection of $V(m)^{p^{e-d}}$ over all $e > d$ is trivial. □

Lemma 2.3. *For every prime ℓ the endomorphism of $\mathcal{F}^{\mathrm{d},+}$ that sends each f to $f^{1-\sigma_\ell}$ is injective.*

Proof. Let f be a non-trivial element of $\mathcal{F}^{\mathrm{d},+}$ and fix a prime p different from ℓ.

By applying Lemma 2.1 with $\Sigma = \mathbb{N}(p)$ we can fix m in $\mathbb{N}(p)$ with $f(m) \neq 1$. Then Lemma 2.2 implies that for some natural number a one has

$$f^{1-\sigma_\ell}(mp^a) = f(mp^a)^{1-\sigma_\ell} \neq 1.$$

This shows that the distribution $f^{1-\sigma_\ell}$ is non-trivial, as required. □

In the sequel we consider the quotient

$$G_n^+ := \mathrm{Gal}(\mathbb{Q}(n)^+/\mathbb{Q})$$

of G_n and write I_n for the annihilator in $\mathbb{Z}[G_n^+]$ of the element

$$\varepsilon_n := (1-\zeta_n)^{1+\tau} \in V(n).$$

of $V(n)$.

In the next result we shall give an explicit description of this ideal in terms of the decomposition behaviour in $\mathbb{Q}(n)^+$ of prime divisors of n. However, before stating this result, we must introduce more notation.

We write $\#X$ for the cardinality of a finite set X. For a finite group Γ we write e_Γ for the idempotent $e_\Gamma := \#\Gamma^{-1} \cdot \sum_{\gamma\in\Gamma} \gamma$ of $\mathbb{Q}[\Gamma]$.

We then obtain an idempotent of $\mathbb{Q}[G_n^+]$ by setting

$$e_n := \begin{cases} e_{G_n^+} + \prod_{\ell|n}(1 - e_{D_{n,\ell}}), & \text{if } n \text{ is a prime power,} \\ \prod_{\ell|n}(1 - e_{D_{n,\ell}}), & \text{otherwise,} \end{cases} \tag{6}$$

where in the products ℓ runs over all prime divisors of n and $D_{n,\ell}$ denotes the decomposition subgroup of ℓ in G_n^+.

For each homomorphism $\psi : G_n \to \mathbb{Q}^{c,\times}$ we write e_ψ for the primitive idempotent $\#G_n^{-1} \sum_{g\in G_n} \psi(g^{-1})g$ of $\mathbb{Q}^c[G_n]$.

For any element u of $V(n)$ we then define $e_\psi \cdot u$ by means of the inclusion $V(n) \subset \mathbb{Q}^c \otimes_{\mathbb{Z}} V(n)$.

Lemma 2.4. *I_n is equal to the set $\{x \in R_n^+ \mid e_n \cdot x = 0\}$.*

Proof. An element x of $\mathbb{Z}[G_n^+]$ belongs to I_n if and only if $x = (1-e)\cdot x$ where the idempotent e is the sum of e_ψ over all homomorphisms $\psi : G_n^+ \to \mathbb{Q}^{c,\times}$ for which $e_\psi \cdot \varepsilon_n \neq 0$. It is therefore enough to show that e is equal to e_n.

If ψ is the trivial homomorphism, then it is easy to check that $e_\psi \cdot \varepsilon_n \neq 0$ if and only if n is a prime power.

On the other hand, if ψ is not trivial, then the distribution relations (4) combine with the fundamental link between cyclotomic elements and first derivatives of Dirichlet L-series (as discussed, for example, in [21, Chap. 3, §5]) to imply that

$$-\frac{1}{2}\sum_{g\in G} \psi(g)^{-1}\log(\sigma_\infty(\varepsilon_n^g)) = L'(\psi^{-1},0)\prod_{\ell\in\mathcal{P}_\psi}(1-\psi(\sigma_\ell^{-1})).$$

Here σ_∞ denotes the embedding $\mathbb{Q}(n) \to \mathbb{C}$ that sends ζ_n to $e^{2\pi i/n}$ and $\mathcal{P}_\psi$ the set of prime divisors of n that do not divide the conductor of ψ.

In particular, since $L'(\psi^{-1},0) \neq 0$, this equality implies that $e_\psi \cdot \varepsilon_n \neq 0$ if and only if the element $e_\psi \cdot \prod_{\ell\in\mathcal{P}_\psi}(1 - e_{D_{n,\ell}}) = e_\psi \cdot \prod_{\ell|n}(1 - e_{D_{n,\ell}})$ is non-zero.

By combining these facts with the explicit definition of e_n one directly checks that $e = e_n$, as required. □

Example 2.5. Lemma 2.4 can be used to extend the explicit computation made by the second author in [18, Prop. 2.4] beyond the special cases that are considered there. For the moment we only record two easy examples.
(i) If n is a power of a prime p, then $D_{n,p} = G_n^+$ so $e_n = 1$ and hence I_n vanishes.
(ii) If n is not a prime power and there exists a prime divisor p of n such that $D_{n,p} \subseteq D_{n,\ell}$ for all prime divisors ℓ of n, then $e_n = 1 - e_{D_{n,p}}$ and so $I_n = \mathbb{Z}[G_n^+] \cdot \sum_{g\in D_{n,p}} g$.

Remark 2.6. Fix f in $\mathcal{F}^{\mathrm{d}}$. Then for every n in $\mathbb{N}^*$ the containment (5) implies $f(n)^{1+\tau}$ belongs to $V(n)$, whilst the relations (4) combine with the argument of Lemma 2.4 to imply that $f(n)^{1+\tau} = e_n \cdot f(n)^{1+\tau}$ in $\mathbb{Q} \otimes_{\mathbb{Z}} V(n)$. In particular, since for every homomorphism $\psi : G_n^+ \to \mathbb{Q}^{c,\times}$ with $e_\psi \cdot e_n \neq 0$ one has both $e_\psi \cdot \varepsilon_n \neq 0$ and $\dim_{\mathbb{Q}^c}\big(e_\psi(\mathbb{Q}^c \otimes_{\mathbb{Z}} V(n))\big) = 1$ (by Dirichlet's Unit Theorem), there exists an element $j_{f,n}$ of $\mathbb{Q}[G_n^+]e_n$ such that $f(n)^{1+\tau} = \varepsilon_n^{j_{f,n}}$ in $\mathbb{Q} \otimes_{\mathbb{Z}} V(n)$.

Remark 2.7. The result of Lemma 2.4 concerns Galois relations between cyclotomic numbers in real abelian fields and so is, in principle, well-known (see, for example, the article of Solomon [20] and the references contained therein). However, the precise nature of the result of Lemma 2.4 will play an important role in later arguments and so we have given a direct proof.

2.3. In this section we collect together several general remarks concerning distributions.

Remark 2.8. If f in $\mathcal{F}^{\rm d}$ is non-trivial, then for every prime p, there exists an m in $\mathbb{N}(p)$ with $f(m) \neq 1$ (this follows from Lemma 2.1 with $\Sigma = \mathbb{N}(p)$). However, for any given finite set of prime numbers $\mathcal{P}$ there exists a non-trivial $f_{\mathcal{P}}$ in $\mathcal{F}^d$ with the property that $f_{\mathcal{P}}(\ell^m) = 1$ for all $\ell \in \mathcal{P}$ and $m \in \mathbb{N}$. In fact, for any non-trivial f in $\mathcal{F}^{\rm d,+}$ the distribution $f_{\mathcal{P}} := (\prod_{\ell \in \mathcal{P}}(1-\sigma_\ell))(f)$ has the required property and is non-trivial by Lemma 2.3.

Remark 2.9. If one fixes a prime p, then one can formulate a natural p-adic analogue of the conjectural equality (3) by defining $\mathcal{F}^{\rm d,p}$ just as $\mathcal{F}^{\rm d}$ except that for each n in $\mathbb{N}^*$ the condition (5) is replaced by $f(n) \in \mathbb{Z}_p \otimes_{\mathbb{Z}} E(n)'$ and then asking if the quotient of $\mathcal{F}^{\rm d,p}$ by its torsion subgroup is generated over the pro-p completion $\widehat{R}^p$ of R by Φ? However, this question has a negative answer. For example, if one fixes any prime ℓ different from p, then the assignment

$$f_\ell(n) := \begin{cases} n^{-1} \otimes \ell, & \text{if } n \text{ is a power of } \ell, \\ 1, & \text{otherwise,} \end{cases}$$

gives a well-defined, non-torsion, element f_ℓ of $\mathcal{F}^{\rm d,p}$ and Lemma 2.1 (with $\Sigma = \mathbb{N}(p)$) implies that f_ℓ does not belong to $\widehat{R}^p \cdot \Phi$.

We finally give an example of a norm-compatible family of global units in the cyclotomic $\mathbb{Z}_p$-extension of a cyclotomic field that cannot arise as the restriction of a distribution.

To describe this we fix distinct odd primes p and q and for each b in $\mathbb{N}$ we set $\Gamma_b := G_{qp^b}^+$ and we choose an element T_b of R that projects to the element $\sum_{g \in \Gamma_b} g$ of $\mathbb{Z}[\Gamma_b]$. For each a in $\mathbb{N}^*$ we then set $\Pi_a := \sum_{b=1}^{b=a-1} T_b$.

Lemma 2.10.

- (i) *The family* $((\varepsilon_{qp^a})^{\Pi_a})_{a\geq 2}$ *is norm-compatible.*
- (ii) *If* $q-1$ *is not divisible by the order of* q *modulo* p*, then there is no* f *in* $\mathcal{F}^d$ *such that* $f(qp^a) = (\varepsilon_{qp^a})^{\Pi_a}$ *for all* $a \geq 2$.

Proof. Claim (i) follows easily from the fact that for $a \geq 2$ one has $\varepsilon_{qp^a}^{T_a} = \mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(qp^a)^+}(\varepsilon_{qp^a}) = 1$.

To prove claim (ii) we argue by contradiction and thus assume that there exists f in $\mathcal{F}^{\rm d}$ with $f(qp^a) = (\varepsilon_{qp^a})^{\Pi_a}$ for all $a \geq 2$. Then for all such a one would have

$$(\varepsilon_{p^a})^{\Pi_a(\sigma_q - 1)} = \mathrm{N}_{p^a}^{qp^a}((\varepsilon_{qp^a})^{\Pi_a}) = \mathrm{N}_{p^a}^{qp^a}(f(qp^a)) = f(p^a)^{\sigma_q - 1}$$

and hence there would exist a non-zero element x_a of the fixed subfield, L say, of $\bigcup_a \mathbb{Q}(p^a)$ by σ_q with

$$(\varepsilon_{p^a})^{\Pi_a} = x_a \cdot f(p^a). \tag{7}$$

Fix t in $\mathbb{N}$ and a in $\mathbb{N}$ with $L \subseteq \mathbb{Q}(p^a)$. Then, by comparing (7) to the image under $\mathrm{N}^{p^{a+t}}_{p^a}$ of the corresponding equality with a replaced by $a+t$, and using the fact that the elements $\{f(p^a)\}_a$ are norm compatible, one finds that $x_{a+t}^{p^t} = (p^{q-1})^{\sum_{i=0}^{i=t-1} p^i} \cdot x_a$ and hence that

$$p^t \cdot v_L(x_{a+t}) = (q-1)(\sum_{i=0}^{i=t-1} p^i) v_L(p) + v_L(x_a) = (q-1)v_L(p)\frac{p^t-1}{p-1} + v_L(x_a),$$

where $v_L(-)$ is the valuation on L at the unique prime above p.

Now the stated assumption on $q-1$ implies that $(q-1)v_L(p) = r + s(p-1)$ for integers r and s that satisfy $0 < r < p-1$ and $s \geq 0$. In this case, therefore, one finds that for all sufficiently large t the above equality implies that

$$\begin{cases} -v_L(x_a) \equiv r\frac{p^t-1}{p-1} - s \pmod{p^t}, & \text{if } v_L(x_a) \leq 0 \\ v_L(x_a) \equiv p^t - r\frac{p^t-1}{p-1} + s \pmod{p^t}, & \text{if } v_L(x_a) > 0. \end{cases}$$

But, since $0 < r < p-1$, it is easily shown that no such integer $v_L(x_a)$ can exist. □

3. Circular distributions and Euler systems

In this section we will establish a close link between the values of distributions in the groups $\mathcal{F}^{\mathrm{d}}$ and $\mathcal{F}^{\mathrm{c}}$.

The precise result is perhaps itself of some interest and will also later play a key role in the construction of the homomorphism κ that occurs in Theorem 1.2.

3.1. For an abelian group A we write A_{tor} for its torsion subgroup and A_{tf} for the quotient of A by A_{tor}. For each prime ℓ we set $A_\ell := \mathbb{Z}_\ell \otimes_{\mathbb{Z}} A$.

For a natural number n we set $\varphi(n) := \#G_n$. We also write $\mathbb{Z}_{(n)}$ and $\mathbb{Z}_{\{n\}}$ for the subrings of $\mathbb{Q}$ that are obtained by intersecting the ℓ-localisations $\mathbb{Z}_{(\ell)}$ of $\mathbb{Z}$ over all primes ℓ that divide n and over all primes ℓ that either divide n or are coprime to $\varphi(n)$ respectively. We note, in particular, that $\mathbb{Z}_{\{n\}}$ is a subring of $\mathbb{Z}_{(n)}$.

We can now state the main result of this section.

Theorem 3.1. *Fix a natural number m. Then for each function f in $\mathcal{F}^{\mathrm{d}}_{(m)}$ and each n in $\mathbb{N}(m)$ there exists an element $r_{f,n}$ of $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} R_n$ such that $f(n) = \Phi(n)^{r_{f,n}}$ in $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} E(n)'$. If f belongs to $\mathcal{F}^{\mathrm{sd}}_{(m)}$, then one can take each element $r_{f,n}$ to belong to $\mathbb{Z}_{\{n\}} \otimes_{\mathbb{Z}} R_n$.*

This result is a considerable strengthening of the main results of the second author in [15] and [16] in that it considers the ℓ-primary properties of the values of distributions at integers n for which $\varphi(n)$ can be divisible by ℓ.

In Corollary 3.4 we will also show Theorem 3.1 implies that any given distribution has 'cyclotomic values' if and only if it has the same Galois descent properties as do cyclotomic units.

3.2. There are two differing notions of 'Euler system' that are useful for us since they are respectively related to the groups of distributions $\mathcal{F}^{\rm sd}$ and $\mathcal{F}^{\rm d}$.

For the reader's convenience we now recall the basic facts concerning these notions.

3.2.1. To describe the first we write $\mathcal{J}(m)$ for each natural number m for the set of positive square-free integers that are only divisible by primes congruent to 1 modulo m.

Then an Euler system over the field $\mathbb{Q}(m)$ is defined by Rubin in [11, §1] to be a map

$$\varepsilon : \mathcal{J}(m) \to \mathbb{Q}^{c,\times}$$

that satisfies the following four conditions for each r in $\mathcal{J}(m)$ and each prime divisor ℓ of r:

(ES$_1$) $\varepsilon(r)$ belongs to $\mathbb{Q}(mr)^\times$.
(ES$_2$) $\varepsilon(r)$ belongs to $E(mr)$ if $r > 1$.
(ES$_3$) $\mathrm{N}^r_{r/\ell}(\varepsilon(r)) = \varepsilon(r/\ell)^{\sigma_\ell - 1}$.
(ES$_4$) $\varepsilon(r) \equiv \varepsilon(r/\ell)$ modulo all primes above ℓ.

For each f in $\mathcal{F}_{(m)}$ and each ζ in μ^*_∞, we define $\varepsilon_{f,\zeta}$ to be the function on $\mathcal{J}(m)$ obtained by setting

$$\varepsilon_{f,\zeta}(m') := f(\zeta \cdot \prod_{\ell | m'} \zeta_\ell)$$

for each m' in $\mathcal{J}(m)$.

Coleman observed that if f belongs to $\mathcal{F}^{\rm sd}_{(m)}$ and ζ to μ_m, then the second distribution relation in (4) combines with the congruence property (2) to imply $\varepsilon_{f,\zeta}$ is an Euler system over $\mathbb{Q}(m)$ in the above sense (cf. [15, Lem. 4.1]).

In addition, the first relation in (4) implies that for any m the elements $\varepsilon_{f,\zeta_{mp^i}}(1) = f(\zeta_{mp^i})$ form a norm-compatible family as i varies over the natural numbers.

However, if f belongs only to $\mathcal{F}^{\rm d}_{(m)}$ then for any ζ in μ_m the function $\varepsilon_{f,\zeta}$ need not be an Euler system in the above sense since a failure of f to satisfy the congruence property (2) means that $\varepsilon_{f,\zeta}$ need not satisfy the condition (ES$_4$).

For this reason we are led to consider an alternative definition of Euler system.

3.2.2. For each natural number m we write $\mathcal{R}(m)$ for the set of square-free products of primes that do not divide m.

To describe the second notion of Euler system we fix a prime p and, for each r in $\mathcal{R}(p)$, we write $\mathbb{Q}(r)^p$ for the composite over all primes divisors ℓ of r of the maximal totally real subextension of $\mathbb{Q}(\ell)$ that has p-power degree over $\mathbb{Q}$. We note, in particular, that for any natural number m prime to r the field $\mathbb{Q}(mr)$ is an extension of $\mathbb{Q}(m)\mathbb{Q}(r)^p$ of degree prime to p.

We now fix a multiple m of p. Then for each function f in $\mathcal{F}_{(m)}$ and each natural number t we define a function $\varepsilon_{f,t}$ on $\mathcal{R}(m)$ by setting

$$\varepsilon_{f,t}(r) := \mathrm{Norm}_{\mathbb{Q}(p^t mr)/\mathbb{Q}(p^t m)\mathbb{Q}(r)^p}(f(p^t mr)).$$

Then, if f belongs to $\mathcal{F}^{\rm d}_{(m)}$, the distribution relation (4) implies that, as t varies over all natural numbers, the collection of functions $\varepsilon_{f,t}$ constitutes an Euler system in the sense defined by Rubin in [13, Def. 2.1.1 and Rem. 2.1.4] for the data $K = \mathbb{Q}(m), \mathcal{N} = \{p\}$,

$T = \mathbb{Z}_p(1)$ and with K_∞ taken to be the union of the fields $\mathbb{Q}(p^t m)$ for $t \geq 1$. (See [13, §3.2] for an explicit description of the cohomology groups that occur in this case.)

In particular, if f belongs to $\mathcal{F}^{\mathrm{d}}_{(p)}$, then the argument of [13, Cor. 4.8.1 and Exam. 4.8.2] shows that for each m in $\mathbb{N}(p)$, each r in $\mathcal{R}(m)$ and each prime ℓ that does not divide mr there exists an integer t that is prime to p and is such that

$$f(\zeta_\ell \cdot \zeta_{mr})^t \equiv f(\zeta_{mr})^t \text{ modulo all primes above } \ell. \tag{8}$$

This observation implies, in particular, that for any f in $\mathcal{F}^{\mathrm{d}}_{(p)}$, any m in $\mathbb{N}(p)$ and any ζ in μ_m, the function $\varepsilon_{f,\zeta}$ defined in §3.2.1 satisfies the conditions (ES_1), (ES_2), (ES_3) and a variant $(\mathrm{ES}_4)_p$ of the condition (ES_4) in which the necessary congruences are only valid after projecting from the appropriate residue fields to their p-primary components.

3.2.3. Finally we recall some basic facts concerning cyclotomic units.

For each n in $\mathbb{N}^*$ the group of 'circular numbers' in $\mathbb{Q}(n)$ is defined by Sinnott [19] to be the subgroup of $\mathbb{Q}(n)^\times$ given by

$$C'(n) := \{(1-\zeta)^r : \zeta \in \mu_n^*, r \in R_n\}$$

and that the group $C(n) := C'(n) \cap E(n)$ of 'cyclotomic units' has finite index in $E(n)$.

It is clear that for any m in $\mathbb{N}(n)$ one has $E(n) \subseteq E(m)$ and $C(n) \subseteq C(m)$. The following observation of Gold and Kim concerning the induced map $E(n)/C(n) \to E(m)/C(m)$ will play a key role in our argument.

Lemma 3.2. *For each n in $\mathbb{N}^*$ and each m in $\mathbb{N}(n)$, one has $C(n) = H^0(G_n^m, C(m))$ and hence the natural map $E(n)/C(n) \to E(m)/C(m)$ is injective.*

Proof. See [4, Cor. 3]. □

3.3. As an important preliminary to the proof of Theorem 3.1, in this section we shall prove a technical result about inverse limits of cyclotomic units.

To do this we fix a prime p and set

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

For any multiple m of p^* we then define the group of 'unit-valued distributions of level (p,m)' to be the R-submodule $\mathcal{F}^{\mathrm{ud}}_{(p,m)}$ of $\mathcal{F}^{\mathrm{d}}$ comprising maps f with the property that for every non-negative integer t one has $f(mp^t) \in E(mp^t)$. We note, in particular, that if m is not a power of p, then (5) implies that $\mathcal{F}^{\mathrm{ud}}_{(p,m)} = \mathcal{F}^{\mathrm{d}}$.

For each non-negative integer t we then write $\mathcal{F}^{\mathrm{u}}(mp^t)$ for the R_{mp^t}-submodule of $E(mp^t)$ that is generated by the set $\{f(\zeta) : f \in \mathcal{F}^{\mathrm{ud}}_{(p,m)}, \zeta \in \mu^*_{mp^t}\}$.

With this definition, the inclusion $\mathcal{F}^{\mathrm{c}} \subseteq \mathcal{F}^{\mathrm{d}}$ implies $C(mp^t) \subseteq \mathcal{F}^{\mathrm{u}}(mp^t)$ and, in addition, it is also clear that for each $t' \geq t$ the following two properties are satisfied

$$\begin{cases} \text{the inclusion } E(mp^t) \subseteq E(mp^{t'}) \text{ restricts to a map } \mathcal{F}^{\mathrm{u}}(mp^t) \subseteq \mathcal{F}^{\mathrm{u}}(mp^{t'}), \\ \text{the norm map } \mathrm{N}^{mp^{t'}}_{mp^t} \text{ restricts to a map } \mathcal{F}^{\mathrm{u}}(mp^{t'}) \to \mathcal{F}^{\mathrm{u}}(mp^t). \end{cases} \tag{9}$$

In the following result we set

$$\mathcal{F}^{\mathrm{u}}(m)_p^\infty := \varprojlim_{a\ge 0} \mathcal{F}^{\mathrm{u}}(mp^a)_p \quad \text{and} \quad C(m)_p^\infty := \varprojlim_{a\ge 0} C(mp^a)_p,$$

where in both cases the transition maps are induced by the norms $\mathrm{N}_{mp^a}^{mp^{a+1}}$.

Proposition 3.3. *For any multiple m of p^* the natural inclusion map $C(m)_p^\infty \to \mathcal{F}^{\mathrm{u}}(m)_p^\infty$ is bijective.*

Proof. We claim first it is enough to show that the quotient group $Q := \mathcal{F}^{\mathrm{u}}(m)_p^\infty/C(m)_p^\infty$ is finite.

To see this we note that, since p^* divides m, we may fix a topological generator γ of $\mathrm{Gal}(\mathbb{Q}(mp^\infty)/\mathbb{Q}(m))$. Then, if Q is finite, there is a natural number t_0 such that for any $t \ge t_0$ the element γ^{p^t} acts trivially on $\mathcal{F}^{\mathrm{u}}(m)_p^\infty/C(m)_p^\infty$. For any $t_1 \ge t_0$ we can then consider the composite homomorphism

$$\theta_{t_0}^{t_1} : (\mathcal{F}^{\mathrm{u}}(mp^{t_1})/C(mp^{t_1}))_p \to (\mathcal{F}^{\mathrm{u}}(mp^{t_0})/C(mp^{t_0}))_p \to (\mathcal{F}^{\mathrm{u}}(mp^{t_1})/C(mp^{t_1}))_p,$$

where the first map is induced by field-theoretic norm and the second by the relevant case of the homomorphism in Lemma 3.2. In particular, since the latter homomorphism is injective the composite sends each x to $\sum_{a=0}^{a=t_1-t_0}(\gamma^{p^{t_0+a}})^m(x)$.

Thus, if $p^{t_1-t_0} \ge \#Q$, then for any x in the projection of Q to $(\mathcal{F}^{\mathrm{u}}(mp^{t_0})/C(mp^{t_0}))_p$ one has $\theta_{t_0}^{t_1}(x) = p^{t_1-t_0+1}\cdot x = 0$ and hence Q vanishes, as claimed.

We next write $E(m)_p^\infty$ for the inverse limit of the groups $E(mp^t)_p$ for $t \ge 0$ with respect to the maps $\mathrm{N}_{mp^t}^{mp^{t+1}}$. We recall that the main result of Greither in [8] (and the earlier work of Kuz'min in [10]) imply that the quotient module $E(m)_p^\infty/C(m)_p^\infty$ is finitely generated over $\mathbb{Z}_p$.

This observation implies that Q is also finitely generated over $\mathbb{Z}_p$ and hence is finite if and only if the space $Q[1/p]$ vanishes.

To study this space we write m' for the maximal divisor of m prime to p and use the algebra $\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}(m'p^\infty)/\mathbb{Q})]]$.

We note that any choice of topological generator of $\mathrm{Gal}(\mathbb{Q}(m'p^\infty)/\mathbb{Q}(m'p))$ induces a natural identification of algebras

$$\Lambda[1/p] = \bigoplus_{\psi\in\Xi} \Lambda_\psi[1/p]$$

where Ξ denotes a set of representatives of the $\mathrm{Gal}(\mathbb{Q}_p^c/\mathbb{Q}_p)$-conjugacy classes of homomorphisms $G_{m'p} \to \mathbb{Q}_p^{c,\times}$ and we set $\Lambda_\psi := \mathbb{Z}_p[\psi][[T]]$.

For any Λ-module N there is a corresponding direct sum decomposition of $\Lambda[1/p]$-modules $N[1/p] = \bigoplus_{\psi\in\Xi} N_\psi[1/p]$ where we write $N_\psi := N \otimes_{\mathbb{Z}_p[G(m'p)]} \mathbb{Z}_p[\psi]$, regarded as a module over Λ_ψ in the obvious way.

It is therefore enough to show that each module $Q_\psi[1/p]$ vanishes and to do this we use the natural exact sequence

$$0 \to Q_\psi[1/p] \to (E(m)_p^\infty/C(m)_p^\infty)_\psi[1/p] \to (E(m)_p^\infty/\mathcal{F}^{\mathrm{u}}(m)_p^\infty)_\psi[1/p] \to 0. \tag{10}$$

If ψ is an odd character of $G_{m'p}$, then all modules in this sequence vanish. This is because in this case each module is invariant under the action of $1-\tau$ and for each non-negative integer i and each u in $E(mp^i)$ the element $u^{2(1-\tau)}$ has finite order (by [22, Th. 4.12]) and hence belongs to $C(mp^i)$.

To deal with the case that ψ is even we write X_m^p for the inverse limit $\varprojlim_i \mathrm{Cl}(\mathbb{Q}(mp^i))_p$ with respect to the natural norm maps. In this case the result [7, Th. 3.1] of Greither (see also the comment at the bottom of [8, p. 120]) shows the existence of an integer a for which there is an equality of characteristic ideals

$$\mathrm{char}_{\Lambda_\psi}((E(m)_p^\infty/C(m)_p^\infty)_\psi) = \pi_\psi^a \cdot \mathrm{char}_{\Lambda_\psi}(X_{m,\psi}^p), \tag{11}$$

where π_ψ is a uniformizer of $\mathbb{Q}_p(\psi)$.

We next note that for any $f \in \mathcal{F}^{\mathrm{ud}}_{(p,m)}$, any non-negative t and any $\zeta \in \mu^*_{mp^t}$ the observations made at the end of §3.2.2 imply that $f(\zeta)$ is equal to the value at 1 of a unit-valued function $\varepsilon_{f,\zeta}$ from $\mathcal{J}(mp^t)$ to $\mathbb{Q}^{c,\times}$ that satisfies the conditions (ES_1), (ES_2), (ES_3) and $(\mathrm{ES}_4)_p$.

These functions $\varepsilon_{f,\zeta}$ may therefore fail to be an Euler system in the strict sense of [13, §1]. However, this failure is immaterial to us since the only place that the condition (ES_4) is used in [13] is in the argument of Kolyvagin that proves [13, Prop. 2.4] and this argument applies the map φ_ℓ that is constructed in [13, Lem. 2.3].

In particular, if one takes the integer M in loc cit. to be a power of p (which is the relevant case for us), then φ_ℓ factors through the projection of $(\mathcal{O}_F/\ell\mathcal{O}_F)^\times$ to its maximal quotient of p-power order and hence it is sufficient to replace (ES_4) by the weaker condition $(\mathrm{ES}_4)_p$.

Given this observation, the proof of [7, Th. 3.1] shows that in Λ_ψ the ideal $\mathrm{char}_{\Lambda_\psi}(X^p_{m,\psi})$ divides $\mathrm{char}_{\Lambda_\psi}((E(m)_p^\infty/\mathcal{F}^{\mathrm{u}}(m)_p^\infty)_\psi)$.

Combining this fact with the equality (11) one deduces that the characteristic ideal over Λ_ψ of the kernel of the natural projection map $(E(m)_p^\infty/C(m)_p^\infty)_\psi \to (E(m)_p^\infty/\mathcal{F}^{\mathrm{u}}(m)_p^\infty)_\psi$ is generated by a power of π_ψ and hence that this kernel has finite exponent.

Taken in conjunction with the exact sequence (10), this last fact implies that the module $Q_\psi[1/p]$ vanishes, as required to complete the proof. □

3.4. We are now ready to prove Theorem 3.1. To do this we fix f in $\mathcal{F}^{\mathrm{d}}_{(m)}$ and n in $\mathbb{N}(m)$.

Writing $D(n)$ for the R_n-module generated by $1-\zeta_n$, we need to prove that $f(n)$ belongs to $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} D(n)$ and to $\mathbb{Z}_{\{n\}} \otimes_{\mathbb{Z}} D(n)$ for each f in $\mathcal{F}^{\mathrm{sd}}_{(m)}$.

Thus, since no prime divisor of n is invertible in $\mathbb{Z}_{(n)}$, the proof of [17, Th. 2.4] implies that it is actually enough to show $f(n)$ belongs to $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} C'(n)$, respectively to $\mathbb{Z}_{\{n\}} \otimes_{\mathbb{Z}} C'(n)$.

To do this we note at the outset that the element $-\zeta_n = (1-\zeta_n)^{1-\tau}$ of $C'(n)$ is a generator of the torsion subgroup W_n of $\mathbb{Q}(n)^\times$ except if $n = 2n'$ with n' odd in which case one has $\mathbb{Q}(n) = \mathbb{Q}(n')$, $W_n = W_{n'}$, and $f(n) = f(n')^{1-\sigma_2}$ as a consequence of (4).

It is therefore enough to prove that for every n the image of $f(n)$ in $V_n := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}(n)^\times$ belongs to $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} C'(n)_{\mathrm{tf}}$ and to $\mathbb{Z}_{\{n\}} \otimes_{\mathbb{Z}} C'(n)_{\mathrm{tf}}$ if f belongs to $\mathcal{F}^{\mathrm{sd}}_{(m)}$.

Now $\mathbb{Z}_{(n)} \otimes_{\mathbb{Z}} C'(n)_{\mathrm{tf}}$ and $\mathbb{Z}_{\{n\}} \otimes_{\mathbb{Z}} C'(n)_{\mathrm{tf}}$ are respectively equal to the intersections in V_n of $\mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} C'(n)_{\mathrm{tf}}$, as p runs over all primes that divide n and over all primes that either divide n or are prime to $\varphi(n)$.

We are therefore reduced to proving that for each such p one has in $E(n)'_{\mathrm{tf},p}$ a containment

$$f(n) \in C'(n)_{\mathrm{tf},p}. \tag{12}$$

Since this result is obvious when $n = 2$ we will also assume in the sequel that $n > 2$ and hence that $\varphi(n)$ is even.

3.4.1. In the case that f belongs to $\mathcal{F}^{\mathrm{sd}}_{(m)}$ and p is prime to both n and $\varphi(n)$ (and hence is odd), the containment (12) is well-known.

To explain this we write G_n^* for the group $\mathrm{Hom}(G_n, \mathbb{Q}_p^{c,\times})$ and we fix a finite extension of $\mathbb{Q}_p$, with valuation ring $\mathcal{O}$, that contains the image of all homomorphisms in G_n^*.

Then for any G_n-module X there is a direct sum decomposition of $\mathcal{O}[G_n]$-modules

$$\mathcal{O} \otimes_{\mathbb{Z}} X = \bigoplus_{\chi \in G_n^*} X^\chi$$

where X^χ denotes the χ-isotypic component $\{x \in \mathcal{O} \otimes_{\mathbb{Z}} X : g(x) = \chi(g) \cdot x \text{ for all } g \in G_n\}$.

If $\chi(\tau) = -1$, then $(E(n)'_{\mathrm{tf}})^\chi$ vanishes, whilst if χ is trivial it is easily checked that $(E(n)'_{\mathrm{tf}})^\chi \subseteq C'(n)^\chi_{\mathrm{tf}}$.

It is therefore enough to prove that for each non-trivial χ with $\chi(\tau) = 1$ the image of $f(n)$ in $(E(n)')^\chi$ is contained in $C'(n)^\chi$. We therefore now fix such a χ.

We write U_n for the unit group of the field $\mathbb{Q}(n)$ and $\mathfrak{E}_n$ for the R_n-submodule of $\mathbb{Q}(n)^\times$ that is generated by the values at 1 of all Euler systems over $\mathbb{Q}(n)$ of the form $\varepsilon_{h,\zeta}$, with h in $\mathcal{F}^{\mathrm{sd}}_{(n)}$ and ζ in μ_n, as discussed in §3.2.1.

Then, since both $f(n)$ and $C'(n)$ are contained in $\mathfrak{E}_n$ it is enough to prove that $\mathfrak{E}_n^\chi$ is contained in $C'(n)^\chi$.

Now, the $\mathcal{O}$-modules $\mathfrak{E}_n^\chi$, U_n^χ and $C'(n)^\chi$ are all free of rank one and, since χ is non-trivial, one has $\mathfrak{E}_n^\chi \subseteq U_n^\chi$.

The required inclusion is therefore a direct consequence of the fact that

$$\mathrm{char}_{\mathcal{O}}\big(U_n^\chi/\mathfrak{E}_n^\chi\big) \subseteq \mathrm{char}_{\mathcal{O}}\big(\mathrm{Cl}(\mathbb{Q}(n))^\chi\big) = \mathrm{char}_{\mathcal{O}}\big(U_n^\chi/C'(n)^\chi\big).$$

Here we write $\mathrm{char}_{\mathcal{O}}(X)$ for the order ideal of a finite $\mathcal{O}$-module X and $\mathrm{Cl}(\mathbb{Q}(n))$ for the ideal class group of $\mathbb{Q}(n)$. In addition, the displayed inclusion follows from the argument used by Rubin to prove [12, Th. 3.2] and the fact that $\mathbb{Q}(n) \cap \mathbb{Q}(p) = \mathbb{Q}$ since we are assuming that p is prime to n, and the displayed equality is true as a consequence of the known validity of the Gras Conjecture (which was shown by Greenberg in [6] to follow from the Main Conjecture of Iwasawa Theory for abelian fields, as subsequently proved, for example, by Mazur and Wiles).

3.4.2. It is now enough to prove (12) in the case that f belongs to $\mathcal{F}^{\mathrm{d}}$ (but not necessarily to $\mathcal{F}^{\mathrm{sd}}$) and that p divides n.

In addition, if $p = 2$ and $n = 2m$ with m odd, then the distribution relation (4) implies both that $f(n) = \mathrm{N}_n^{2n}(f(2n))$ and that $\mathrm{N}_n^{2n}(C'(2n)) \subseteq C'(n)$.

It is therefore enough to prove (12) in the case that n is divisible by p^*, as is required to apply Proposition 3.3.

We assume first that n is not a power of p and so is divisible by at least two primes. In this case the restriction of f to $\mathbb{N}(n)$ is unit-valued (by (5)) and so $\{f(p^i n)\}_{i\geq 0}$ belongs to the limit $\mathcal{F}^{\mathrm{u}}(n)_p^\infty$ that occurs in Proposition 3.3.

The latter result therefore implies that $\{f(p^i n)\}_{i\geq 0}$ belongs to $C(n)_p^\infty$ and hence that $f(n)$ belongs to $C(n)_p$, as required.

If now n is a power of p, then we set $a_p := 2$ if $p = 2$ and $a_p = 0$ if $p \neq 2$. We then fix an element γ of $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q}(p^{a_p}))$ that restricts to give a generator of $\mathrm{Gal}(\mathbb{Q}(p^\infty)/\mathbb{Q}(p^{a_p}))$ and define a function f_γ on $\mathbb{N}(n)$ by setting $f_\gamma(n') := f(n')^{\gamma-1}$ for all multiples n' of n.

Then this function f_γ belongs to $\mathcal{F}^{\mathrm{ud}}_{(p,m)}$ and so the same argument as above shows that $f_\gamma(n) = f(n)^{\gamma_n - 1}$ belongs to $C(n)_p$, where we write γ_n for the image of γ in G_n.

Now, since n is a power of p, this implies the existence of an element r_n of $R_{n,p}$ with

$$f(n)^{\gamma_n - 1} = (1-\zeta_n)^{r_n}.$$

Further, since the norm to $\mathbb{Q}(p^{a_p})$ of this element is trivial, one has $r_n = (\gamma_n - 1)\cdot r'_n$ for some element r'_n of $R_{n,p}$ and it is enough to show that the element

$$x := f(n)/(1-\zeta_n)^{r'_n}$$

belongs to $C(n)_p$. Note also that x belongs to the p-completion of the group of p-units in $\mathbb{Q}(p^{a_p})$ as a consequence of (5).

In particular, if $p \neq 2$, then x has the form $\pm p^b$ for some b in $\mathbb{Z}_p$ and it is enough to note that both $-1 = (1-\zeta_n)^{n(1-\tau)}$ and $p = (1-\zeta_n)^{\sum_{g\in G_n} g}$ belong to $C(n)$.

If, lastly, $p = 2$, then there are elements a and b of $\mathbb{Z}_p$ such that $x = i^a(1-i)^b$. To deal with this case we can also assume, without loss of generality, that $\zeta_4 = i$.

Then if $n = 4$, it is enough to note that $i = (1-\zeta_n)^{\tau-1}$ and $1 - i = 1 - \zeta_n$ belong to $C(4)$. Similarly, if n is divisible by 8, then the containment $x \in C(n)_p$ follows from the fact that $i = (1-\zeta_n)^{n(1-\tau)/4}$ and $(1-\zeta_n)^{\sum_{g\in G_n} g} = i^c(1-i)$ for some integer c.

This completes the proof of Theorem 3.1.

3.5. Finally, we show Theorem 3.1 implies that any given distribution in $\mathcal{F}^{\mathrm{d}}$ has 'cyclotomic values' if and only if it has the same Galois descent properties as Lemma 3.2 implies for cyclotomic units.

Corollary 3.4. *Fix a distribution f in $\mathcal{F}^{\mathrm{d}}$. For n in $\mathbb{N}^*$ write $C_f(n)$ for the R_n-submodule of $E(n)$ generated by $C(n)$ together with $(\Phi^{-v_{f,n}}f)(n)$ where $v_{f,n} = 0$ unless $n = p^d$ for some prime p in which case $v_{f,n}$ is the valuation of $f(n)$ at the unique p-adic place of $\mathbb{Q}(n)$.*

Then for every n in $\mathbb{N}^*$ there exists an element $r'_{f,n}$ of R_n such that $f(n) = \Phi(n)^{r'_{f,n}}$ if and only if for all m in $\mathbb{N}^*$ and all m' in $\mathbb{N}(m)$ one has $C_f(m) = H^0(G_m^{m'}, C_f(m'))$.

Proof. Necessity of the given conditions is an immediate consequence of Lemma 3.2 since if $f(m) = \Phi(m)^{r'_{f,m}}$ for some $r'_{f,m}$ in R_m, then $C_f(m) = C(m)$.

For each n we set $f_n := \Phi^{-v_{f,n}}f$. Then to show sufficiency of the stated conditions it suffices, by virtue of the observation made at the beginning of §3.4, to check that for each prime ℓ these conditions imply that $f_n(n)$ belongs to the ℓ-adic completion $C(n)_\ell$ of $C(n)$.

It is thus enough to note that these conditions imply that

$$f_n(n) \in C_f(n)_\ell = H^0(G_n^{n\ell}, C_f(n\ell)_\ell) = H^0(G_n^{n\ell}, C(n\ell)_\ell) = C(n)_\ell$$

where the first equality holds by assumption, the second follows from Theorem 3.1 and the third from Lemma 3.2. □

Remark 3.5. The set $\Sigma := \{n \in \mathbb{N} : \mathbb{Z}_{\{n\}} = \mathbb{Z}\}$ is cofinal in $\mathbb{N}$ (since it contains $d!$ for all d in $\mathbb{N}$) and is also closed under taking powers. We may therefore apply Lemma 2.1 to this set to deduce that any f in $\mathcal{F}^{\mathrm{d}}$ is uniquely determined by its values at integers in Σ. This suggests it is possible that, rather than relying on possible Galois descent properties as in Corollary 3.4, Theorem 3.1 could itself directly imply that for every f in $\mathcal{F}^{\mathrm{sd}}$ and every m in $\mathbb{N}^*$ there exists an element $r'_{f,n}$ of R_n with $f(n) = \Phi(n)^{r'_{f,n}}$.

Remark 3.6. The second author would like to take this opportunity to point out that the proof of the main result of [15] is incorrect as given and further that it seems the argument in loc. cit. can only be corrected either by assuming the sort of Galois descent property on distributions that arises in Corollary 3.4, or by inverting all primes that divide $\varphi(nt)$ but not nt. The point is that [15, Lem. 5.4(i)] claims that the given inverse limits are equal if and only if $\mathfrak{E}_{p,s}(\mu_{p^rs}) = \mathcal{C}_{p^rs}$ for all r and this may not be true since not all elements of $\mathfrak{E}_{p,s}(\mu_{p^rs})$ must be universal norms in $\mathbb{Q}(p^\infty s)/\mathbb{Q}(p^r s)$. A similar issue arises with aspects of the argument used to prove [16, Th. 2.4] but, given the assumptions in loc. cit., the problem in that case can be avoided by using the approach described above in §3.4.1. The second author would like to thank the first author for noticing this.

4. Torsion-valued distributions

In the sequel we shall say that a distribution f in $\mathcal{F}^{\mathrm{d}}$ is 'torsion-valued' if $f(n)$ has finite order for every n in $\mathbb{N}^*$ and we write $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ for the R-submodule of $\mathcal{F}^{\mathrm{d}}$ comprising all such distributions. In particular, it is clear that $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ contains the torsion subgroup $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}}$ of $\mathcal{F}^{\mathrm{d}}$.

We shall now make a detailed study of torsion-valued distributions in order to prove the following result.

In this result, and the sequel, we regard the union $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}(n)$ over n in $\mathbb{N}^*$ as a subfield of $\mathbb{C}$ and write τ for the element of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ induced by complex conjugation.

We also use the R-module $\widehat{\mathbb{Z}}(1)$ defined just prior to the statement of Theorem 1.2.

Theorem 4.1.

(i) *$\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ is equal to $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} + (1-\tau)\mathcal{F}^{\mathrm{c}}$ and is also the kernel of the endomorphism of $\mathcal{F}^{\mathrm{d}}$ that is induced by multiplication by $1+\tau$.*

(ii) *There exist canonical isomorphisms of R-modules*

$$\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}/\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} \cong (1-\tau)\mathcal{F}^{\mathrm{c}} \cong \widehat{\mathbb{Z}}(1).$$

The first of these is induced by the equality $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}} = \mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} + (1-\tau)\mathcal{F}^{c}$ in claim (i) and the second sends $\Phi^{1-\tau}$ to the topological generator $(\zeta_m)_m$ of $\widehat{\mathbb{Z}}(1)$.

(iii) *If $\mathcal{F}^*$ denotes either $\mathcal{F}^{\mathrm{d}}$ or $\mathcal{F}^{\mathrm{sd}}$, then the R-module homomorphism*

$$\mathcal{F}^*_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}} \to (1+\tau)\mathcal{F}^*/(1+\tau)\mathcal{F}^{\mathrm{c}}$$

that is induced by multiplication by $1+\tau$ is bijective.

This result will play a key role in the proof of Theorem 1.2. After establishing several preliminary results concerning various inverse limits, it will be proved in §4.3.

4.1. In the sequel, for each n in $\mathbb{N}^*$ we write $\mathcal{T}_n$ for the annihilator of $-\zeta_n$ in R_n and set

$$\mathcal{T}_n^* := \begin{cases} \mathcal{T}_n, & \text{if } n \text{ is even} \\ \mathcal{T}_{2n}, & \text{if } n \text{ is odd.} \end{cases}$$

We note, in particular, that if n is odd, then $\mathcal{T}_n$ is a submodule of $\mathcal{T}_n^*$ of index 2 (and that $n \in \mathcal{T}_n^* \setminus \mathcal{T}_n$).

Lemma 4.2.

(i) *For any natural number n and prime ℓ, one has $\pi_n^{n\ell}(\mathrm{Ann}_{R_{n\ell}}(\mu_{n\ell})) \subseteq \mathrm{Ann}_{R_n}(\mu_n)$, with equality unless $\ell = 2$ and n is odd.*

(ii) *For any n in $\mathbb{N}^*$ and any m in $\mathbb{N}(n)$ one has $\pi_n^m(\mathcal{T}_m^*) \subseteq \mathcal{T}_n^*$, with equality if $n \in \mathbb{N}(4)$.*

(iii) *The sequence*

$$0 \to \varprojlim_n \mathcal{T}_n^*(1-\tau) \to R(1-\tau) \to \varprojlim_n R_n(1-\tau)/\mathcal{T}_n^*(1-\tau) \to 0$$

is exact, where the inverse limits are taken with respect to the transition maps induced by π_n^m, the second arrow denotes the natural inclusion and the third the natural diagonal map.

Proof. To prove claim (i) we note first that if $\ell = 2$ and n is odd, then $\mathbb{Q}(n\ell) = \mathbb{Q}(n)$ whilst $\mu_n = (\mu_{n\ell})^2$ and so $\mathrm{Ann}_{R_{n\ell}}(\mu_{n\ell})$ is a subgroup of $\mathrm{Ann}_{R_n}(\mu_n)$ of index 2.

To deal with the general case we set $m := n\ell$ and consider the exact commutative diagram of R_m-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ann}_{R_m}(\mu_m) & \longrightarrow & R_m & \xrightarrow{\theta_m} & \mu_m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \pi_n^m} & & \downarrow{\scriptstyle x \mapsto x^\ell} & & \\ 0 & \longrightarrow & \mathrm{Ann}_{R_n}(\mu_n) & \longrightarrow & R_n & \xrightarrow{\theta_n} & \mu_n & \longrightarrow & 0, \end{array}$$

where $\theta_m(1) = \zeta_m$ and $\theta_n(1) = \zeta_n$.

Then π_n^m is surjective and so, by applying the Snake Lemma to this diagram, we find it is enough to prove that $\theta_m(\ker(\pi_n^m)) = \mu_\ell$.

To do this we note $\ker(\pi_n^m)$ is generated over R_m by the set $\{\sigma - 1 : \sigma \in G_n^m\}$ and that an element σ of G_m belongs to G_n^m if and only if $\sigma(\zeta_m) = \zeta_m^{a_\sigma}$ for an integer a_σ with $a_\sigma \equiv 1 \pmod{n}$.

In particular, if ℓ divides n, then there exists an element σ of G_n^m with $a_\sigma = 1 + n$ and $\theta_m(\sigma - 1)$ is equal to the generator $\zeta_m^n = \zeta_\ell$ of μ_ℓ.

If ℓ is prime to n, then the first observation allows us to assume that ℓ is odd. In this case there are at least $\ell - 2$ integers a with $1 \leq a < \ell$ for which $1 + a \cdot n$ is prime to m and, for any such a, the corresponding element σ of G_n^m is such that $\theta_m(\sigma - 1) = \zeta_m^{a \cdot n} = \zeta_\ell^a$ is a generator of μ_ℓ. This proves claim (i).

To prove claim (ii) we can reduce to the case $m = n\ell$ with ℓ prime. Then, after noting that for each natural number t one has

$$\mathcal{T}_t^* := \begin{cases} \mathrm{Ann}_{R_t}(\mu_{t/2}), & \text{if } t \equiv 2 \pmod{4}, \\ \mathrm{Ann}_{R_t}(\mu_t), & \text{otherwise,} \end{cases}$$

the claimed result follows directly from claim (i).

To prove claim (iii) we use the tautological short exact sequences

$$0 \to \mathcal{T}_n^*(1-\tau) \to R_n(1-\tau) \to R_n(1-\tau)/\mathcal{T}_n^*(1-\tau) \to 0.$$

As n varies these sequences are compatible with the transition morphisms that are induced by π_n^m (and the inclusions of claim (ii)). Hence, by passing to the inverse limit we obtain an exact sequence of R-modules

$$\varprojlim_n \mathcal{T}_n^*(1-\tau) \to R(1-\tau) \to \varprojlim_n R_n(1-\tau)/\mathcal{T}_n^*(1-\tau) \to \varprojlim_n^1 \mathcal{T}_n^*(1-\tau),$$

where we have identified $\varprojlim_n R_n(1-\tau)$ with $R(1-\tau)$ in the obvious way.

To deduce claim (iii) it thus suffices to note that the derived limit $\varprojlim_n^1 \mathcal{T}_n^*(1-\tau)$ vanishes since it can be computed by restricting to the cofinal subset $\mathbb{N}(4)$ for which claim (ii) implies that the transition maps $\mathcal{T}_m^*(1-\tau) \to \mathcal{T}_n^*(1-\tau)$ are surjective. □

4.2. In this section we consider functions f in $\mathcal{F}^{\mathrm{d}}$ with the property that for all n in $\mathbb{N}^*$ one has

$$f(n)^{1+\tau} = 1. \tag{13}$$

We recall that $\mathbb{Q}(n)^+$ denotes the maximal totally real subfield of $\mathbb{Q}(n)$ and write $E(n)^+$ for the group of algebraic units $E(n) \cap \mathbb{Q}(n)^+$ in $\mathbb{Q}(n)^+$. We also recall that W_n denotes the torsion subgroup of $E(n)$.

Lemma 4.3. *If f is any distribution with property (13), then for every n in $\mathbb{N}^*$ the element $f(n)$ belongs to the group $\langle -\zeta_n \rangle$ generated by $-\zeta_n$.*

In particular, a distribution f belongs to $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ if and only it has property (13).

Proof. It is clearly enough to prove the first assertion and to do this we first consider the case that $n = p^d$ for some prime p.

In this case the unique prime ideal of $E(n)$ above p is stable under the action of τ and so the given equality (13) combines with the containment (5) to imply that $f(n)$ belongs to $E(n)$.

From the result of [22, Cor. 4.13] we can therefore deduce that $f(n)$ has the form $w \cdot u$ with w in W_n and u an element of $E(n)^+$ that is either trivial or has infinite order. Given this, (13) implies that

$$1 = f(n)^{1+\tau} = w^{1+\tau} u^{1+\tau} = u^2$$

and hence that $u = 1$ and so $f(n) \in W_n$.

Now if $n \neq 2$, then $W_n = \langle -\zeta_n \rangle$ and so we obtain the required claim. In addition, if $n = 2$, then $f(2) = \mathrm{N}_2^4(f(4)) \in \mathrm{N}_2^4(\mu_4) = \{1\} = \langle -\zeta_2 \rangle$.

We can therefore assume that n is not a prime power. In this case (5) implies directly that $f(n)$ belongs to $E(n)$ and then the argument of [22, Cor. 4.13] implies $f(n)$ can be written as $(1-\zeta_n)^a wu$ with $a \in \{0,1\}$, $w \in W_n$ and $u \in E(n)^+$. Then the equality (13) implies that

$$1 = (1-\zeta_n)^{a(1+\tau)} u^2 = \varepsilon_n^a u^2.$$

This implies that ε_n^a, and hence also

$$(-\zeta_n)^a = (1-\zeta_n)^{a(1-\tau)} = (1-\zeta_n)^{a(1+\tau)}(1-\zeta_n)^{-2a\tau} = \varepsilon_n^a (1-\zeta_n^{-1})^{-2a},$$

is a square in $E(n)$. Since the argument of loc. cit. implies $-\zeta_n$ is not a square in $E(n)$ we deduce that $a=0$.

By using the same argument as above we can then deduce that $f(n)=wu$ must belong to W_n.

If $n \not\equiv 2 \pmod 4$, then $W_n = \langle -\zeta_n \rangle$ and we are done. In addition, if $n=2n'$ with n' odd, then

$$f(n) = f(n')^{1-\sigma_2} \in \langle (-\zeta_{n'})^{1-\sigma_2} \rangle = \langle \zeta_{n'} \rangle = \langle -\zeta_n \rangle,$$

as required. □

If f is any distribution with property (13), then Lemma 4.3 implies that for each $n \in \mathbb{N}^*$ there exists an element $r'_n = r'_{f,n}$ of R_n that is well-defined modulo $\mathcal{T}_n$ and is such that

$$f(n) = (1-\zeta_n)^{r'_n(1-\tau)}. \tag{14}$$

In particular, since $\mathcal{T}_n \subseteq \mathcal{T}_n^*$, the image $r_n = r_{n,f}$ in $R_n/\mathcal{T}_n^*$ of any such element r'_n is uniquely determined by f and n.

Proposition 4.4. *For any f in $\mathcal{F}^{\mathrm{d}}$ with property (13) the element $(r_n(1-\tau))_{n\in\mathbb{N}^*}$ belongs to the limit $\varprojlim_n R_n(1-\tau)/\mathcal{T}_n^*(1-\tau)$ that occurs in Lemma 4.2(iii).*

Proof. It suffices to show that for each $n \in \mathbb{N}^*$ and each prime ℓ one has

$$\pi_n^{n\ell}(r'_{n\ell}) \equiv r'_n \ \text{ modulo } \ \mathcal{T}_n^*.$$

If ℓ divides n, then this is true since the first equality in (4) implies that

$$\begin{aligned}(-\zeta_n)^{r'_{n\ell}} = (1-\zeta_n)^{r'_{n\ell}(1-\tau)} &= (\mathrm{N}_n^{n\ell}(1-\zeta_{n\ell}))^{r'_{n\ell}(1-\tau)} \\ &= \mathrm{N}_n^{n\ell}(f(n\ell)) = f(n) = (1-\zeta_n)^{r'_n(1-\tau)} = (-\zeta_n)^{r'_n}.\end{aligned}$$

If n is odd and $\ell=2$, then $\pi_n^{n\ell}$ is the identity map and so it is enough to show that $r'_{n\ell} \equiv r'_n \pmod{\mathcal{T}_n^*}$. But in this case one has $\zeta_{n\ell}^2 = \zeta_n = (\zeta_n^{\sigma_2})^2$ so that $-\zeta_{n\ell} = \zeta_n^{\sigma_2}$ and hence (4) implies

$$\begin{aligned}(\zeta_n)^{r'_{n\ell}\cdot\sigma_2} = (-\zeta_{n\ell})^{r'_{n\ell}} &= (1-\zeta_{n\ell})^{r'_{n\ell}(1-\tau)} = f(n\ell) \\ &= f(n)^{1-\sigma_2} = (1-\zeta_n)^{r'_n(1-\tau)(1-\sigma_2)} = (-\zeta_n)^{r'_n(1-\sigma_2)} = (\zeta_n)^{r'_n\cdot\sigma_2}.\end{aligned}$$

This shows that $r'_{n\ell} \equiv r'_n \pmod{\mathcal{T}_n^*}$, as required.

Finally, to deal with the case that ℓ is odd and prime to n we fix a prime divisor q of n. We note first that, as the natural number b varies, the equality (4) implies that the elements

$$(-\zeta_{nq^b})^{r'_{nq^b}} = (1-\zeta_{nq^b})^{r'_{nq^b}(1-\tau)} = f(nq^b)$$

and

$$(-\zeta_{n\ell q^b})^{r'_{n\ell q^b}} = (1-\zeta_{n\ell q^b})^{r'_{n\ell q^b}(1-\tau)} = f(n\ell q^b)$$

form elements c and c' of $W_\infty := \varprojlim_{b\geq 1} W_{n\ell q^b}$, where the limit is taken with respect to the norms $\mathrm{N}_{n\ell q^b}^{n\ell q^{b'}}$ for $b' \geq b$.

In addition, (4) also implies that for each b one has

$$\begin{aligned}(-\zeta_{nq^b})^{r'_{nq^b}(\ell-1)} &= (1-\zeta_{nq^b})^{(1-\tau)r'_{nq^b}(1-\sigma_\ell)\sigma_\ell^{-1}} = f(nq^b)^{(1-\sigma_\ell)\sigma_\ell^{-1}}\\ &= \mathrm{N}^{n\ell q^b}_{nq^b}(f(n\ell q^b))^{\sigma_\ell^{-1}} = (\mathrm{N}^{n\ell q^b}_{nq^b}(1-\zeta_{n\ell q^b}))^{r'_{n\ell q^b}(1-\tau)\sigma_\ell^{-1}}\\ &= (1-\zeta_{nq^b})^{(\sigma_\ell^{-1}-1)r'_{n\ell q^b}(1-\tau)} = (-\zeta_{nq^b})^{r'_{n\ell q^b}(\ell-1)}.\end{aligned}$$

This implies that the element $c^{-1}c'$ of W_∞ is annihilated by raising to the power $\ell-1$. Since the maximal pro-q quotient of W_∞ is torsion-free this shows that the order of $(-\zeta_n)^{-r'_n+r'_{n\ell}}$ is prime to q.

As q is an arbitrary divisor of n it therefore follows that $(-\zeta_n)^{-r'_n+r'_{n\ell}}$ is equal to 1 if n is even and to either ±1 if n is odd, and hence that $\pi^{n\ell}_n(r'_{n\ell}) \equiv r'_n \pmod{\mathcal{T}^*_n}$, as required. □

4.3. We are now ready to prove Theorem 4.1.

The final assertion of claim (i) follows directly from the final assertion of Lemma 4.3 and it is also clear that $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ contains both $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}}$ and $(1-\tau)\mathcal{F}^{\mathrm{c}}$. To prove claim (i) it is thus enough to show that $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ is contained in $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} + (1-\tau)\mathcal{F}^{\mathrm{c}}$.

To do this we take f in $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}}$ and use the elements $(r'_n)_n$ that arise in the equality (14). Taking account firstly of Proposition 4.4, and then of the exact sequence in Lemma 4.2(iii), we deduce the existence of an element r of R such that, for each $n \in \mathbb{N}^*$, the image of $r(1-\tau)$ in $R_n(1-\tau)$ is equal to $r'_n(1-\tau) + t_n(1-\tau)$ for an element t_n of $\mathcal{T}^*_n$. This implies

$$f(n) = (1-\zeta_n)^{r'_n(1-\tau)} = (1-\zeta_n)^{r(1-\tau)}\cdot(1-\zeta_n)^{t_n(1-\tau)} = \Phi^{(1-\tau)r}(n)\cdot(-\zeta_n)^{t_n}. \tag{15}$$

In particular, since the annihilator $\mathcal{T}_n$ in R_n of $-\zeta_n$ is a submodule of $\mathcal{T}^*_n$ of index at most two, this shows that the distribution $f\cdot\Phi^{-(1-\tau)r}$ has order at most two and hence belongs to $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}}$, as suffices to complete the proof of claim (i).

Since $\mathcal{F}^{\mathrm{c}}$ is torsion-free the intersection $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} \cap \mathcal{F}^{\mathrm{c}}$ is trivial and so the first isomorphism stated in claim (ii) follows directly from the equality $\mathcal{F}^{\mathrm{d}}_{\mathrm{tv}} = \mathcal{F}^{\mathrm{d}}_{\mathrm{tor}} + (1-\tau)\mathcal{F}^{\mathrm{c}}$ that is proved in claim (i).

Write ζ for the topological generator $(\zeta_m)_m$ of $\widehat{\mathbb{Z}}(1)$. Then, to complete the proof of claim (ii), we need to show that the assignment

$$\Phi^{(1-\tau)r} \mapsto \zeta^r \tag{16}$$

for each r in R gives a well-defined isomorphism of R-modules $(1-\tau)\mathcal{F}^c \cong \widehat{\mathbb{Z}}(1)$.

To check this we note first that for any r and r' in R one has

$$\begin{aligned}\Phi^{(1-\tau)r} = \Phi^{(1-\tau)r'} &\iff \Phi^{(1-\tau)(r-r')} = 1\\ &\iff r-r' \in R\cap\prod_n \mathcal{T}_n\\ &\iff r-r' \in \varprojlim_n \mathcal{T}^*_n\\ &\iff \zeta^{r-r'} = 1.\end{aligned}$$

Here the first equivalence is clear, the second follows from the fact that $\Phi^{1-\tau}(n) = -\zeta_n$ for all n, the third from the fact that $R\cap\prod_n\mathcal{T}_n = \varprojlim_n \mathcal{T}^*_n$ since $\mathcal{T}_n = \mathcal{T}^*_n$ for all even n and the final equivalence is true because $\mathcal{T}_n^*$ is equal to the annihilator in R_n of ζ_n whenever n is a multiple of 4.

This shows that the assignment (16) is both well-defined and injective. The proof of claim (ii) is then completed by noting this map is clearly also both surjective and a homomorphism of R-modules.

Next we note that the surjectivity of the map given in claim (iii) is clear since the torsion subgroup of $\mathcal{F}^{\mathrm{d}}$ is annihilated by $1+\tau$.

To prove claim (iii) it is thus enough to show that if f is any element of $\mathcal{F}^*$ such that $f^{1+\tau}$ belongs to $(1+\tau)\mathcal{F}^{\mathrm{c}}$, then f must belong to the subgroup $\mathcal{F}^*_{\mathrm{tor}}+\mathcal{F}^{\mathrm{c}}$.

Now, for any such f there exists an element r of R with $f^{1+\tau}=(\Phi^r)^{1+\tau}$ and so the product distribution $f_1 := f\cdot\Phi^{-r}$ satisfies the condition (13).

By the argument in claim (i) this implies f_1 belongs to $\mathcal{F}^*_{\mathrm{tor}}+(1-\tau)\mathcal{F}^{\mathrm{c}}$ and hence that $f=f_1\cdot\Phi^r$ belongs to $\mathcal{F}^*_{\mathrm{tor}}+(1-\tau)\mathcal{F}^{\mathrm{c}}+\mathcal{F}^{\mathrm{c}}=\mathcal{F}^*_{\mathrm{tor}}+\mathcal{F}^{\mathrm{c}}$, as required.

This completes the proof of Theorem 4.1.

Remark 4.5. The equality (15) and isomorphism (16) combine to give a more conceptual proof of the equality $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}}=\mathcal{D}$ that was discussed in the Introduction and first proved by the second author in [17]. Specifically, the equality (15) shows that for any f in $\mathcal{F}^{\mathrm{d}}_{\mathrm{tor}}$ one has $f=f_1\cdot f_2$ with $f_1\in(1-\tau)\mathcal{F}^{\mathrm{c}}$ and $f_2\in\mathcal{F}^{\mathrm{d}}$ such that $f_2(n)=(-\zeta_n)^{t_n}$ for all n, where each t_n belongs to $\mathcal{T}_n^*$ and so $f_2(n)\in\langle(-1)^n\rangle$. Thus, since $(1-\tau)\mathcal{F}^{\mathrm{c}}$ is torsion-free, it follows that $f=f_2$ is such that $f(n)$ belongs to $\{\pm1\}$ and can be non-trivial only if n is odd. Given this, it is then easy to check directly from the distribution relations (4) that f must be a Coleman distribution δ_Π for a suitable set of odd prime numbers Π.

5. Distributions of prime level

In this section we consider distributions of prime level, as defined in §2.1.2.

5.1. For brevity we set $\overline{\mathcal{F}}^{\mathrm{d}} := (1+\tau)\mathcal{F}^{\mathrm{d}}$ and $\overline{\mathcal{F}}^{\mathrm{c}} := (1+\tau)\mathcal{F}^{\mathrm{c}}$ and for each m in $\mathbb{N}^*$ also $\overline{\mathcal{F}}^{\mathrm{d}}_{(m)} := (1+\tau)\mathcal{F}^{\mathrm{d}}_{(m)}$.

We recall that ι_m denotes the natural restriction map $\mathcal{F}^{\mathrm{d}}\to\mathcal{F}^{\mathrm{d}}_{(m)}$ and we set $\mathcal{F}^{\mathrm{c}}_{(m)} := \iota_m(\mathcal{F}^{\mathrm{c}})$ and $\overline{\mathcal{F}}^{\mathrm{c}}_{(m)} := (1+\tau)\mathcal{F}^{\mathrm{c}}_{(m)}$. For each prime p we then write

$$\kappa_p : \overline{\mathcal{F}}^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}} \to \overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$$

for the homomorphism that is induced by ι_p.

Finally we recall the torsion-free subgroups $V(n)$ of $\mathbb{Q}(n)^{+,\times}$ that are defined in §2.2.

In terms of this notation, we can now state the main result that we prove concerning distributions of prime level.

Theorem 5.1. *For each prime p the following claims are valid.*

(i) *The homomorphism κ_p is injective and its cokernel is annihilated by $1-\sigma_p$.*

(ii) *The quotient group $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$ is uniquely p-divisible.*

(iii) *The following conditions are equivalent.*

  (a) *The quotient group $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}}$ is uniquely p-divisible.*

(b) *If f is any distribution in $\mathcal{F}^{\mathrm{d},+}$ with the property that $f(n) \in V(n)^p$ for all $n \in \mathbb{N}(p)$, then $f(n) \in V(n)^p$ for all n.*

(c) *There exists a natural number t such that if f is any distribution in $\mathcal{F}^{\mathrm{d},+}$ with the property that $f(n) \in V(n)^{p^t}$ for all $n \in \mathbb{N}(p)$, then $f(n) \in V(n)^p$ for all n.*

In Remark 5.6 below we will discuss the explicit condition that occurs in Theorem 5.1(iii)(c) in the context of cyclotomic distributions.

The proof of this result will occupy the rest of §5. In the sequel we shall therefore fix a prime p.

5.2. In this section we prove Theorem 5.1(i).

To verify that κ_p is injective, we fix an f in $\mathcal{F}^{\mathrm{d}}$ such that $\iota_p(f^{1+\tau}) \in (1+\tau)\iota_p(\mathcal{F}^{\mathrm{c}})$ and, under these hypotheses, we must show that $f^{1+\tau} \in (1+\tau)\mathcal{F}^{\mathrm{c}}$.

It is therefore enough to show that if r is any element of R for which $\iota_p(f^{1+\tau}) = \iota_p(\Phi^{r(1+\tau)})$, then one has $f^{1+\tau} = \Phi^{r(1+\tau)}$.

But if we fix such an r then the product distribution $\Delta := f^{1+\tau} \cdot \Phi^{-r(1+\tau)}$ belongs to the module $\mathcal{F}^{\mathrm{d},+}$ defined in §2.2 and also, by assumption, to the kernel of ι_p.

Hence, by applying Lemma 2.1 (with $\Sigma = \mathbb{N}(p)$), we can conclude that Δ is trivial, as required.

To show $\mathrm{cok}(\kappa_p)$ is annihilated by $1-\sigma_p$ it is enough to show that for any given function f in $\mathcal{F}^{\mathrm{d}}_{(p)}$ there exists a function f' in $\mathcal{F}^{\mathrm{d}}$ for which one has $f^{1-\sigma_p} = \iota_p(f')$.

To do this we define f' to be the unique $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$-equivariant map $\mu_\infty^* \to \mathbb{Q}^{c,\times}$ that satisfies

$$f'(\zeta_n) := \begin{cases} f(n)^{1-\sigma_p}, & \text{if } p \text{ divides } n, \\ \mathrm{N}_n^{np}(f(np)), & \text{if } p \text{ is prime to } n. \end{cases}$$

It is then immediately clear that $\iota_p(f') = f^{1-\sigma_p}$ whilst an easy exercise shows that f' inherits the properties (1) and (2) from f and hence that f' belongs to $\mathcal{F}^{\mathrm{d}}$, as required.

This completes the proof of Theorem 5.1(i).

Remark 5.2. The same argument can be used to show that for any natural numbers m and n the natural 'restriction' map $\overline{\mathcal{F}}_{(m)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(m)} \to \overline{\mathcal{F}}_{(mn)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(mn)}$ is injective and has cokernel annihilated by $\prod_\ell(1-\sigma_\ell)$ where ℓ runs over all primes that divide n but not m.

5.3. In this section we prove Theorem 5.1(ii).

5.3.1. For each n in $\mathbb{N}^*$ we set $R_n^+ := \mathbb{Z}[G_n^+]$ and write $D(n)^+$ for the R_n^+-submodule of $V(n)$ that is generated by $\varepsilon_n := (1-\zeta_n)^{1+\tau}$.

We then define $\mathcal{V}_p^{\mathrm{d}}$ to be the subgroup of $\prod_{m \in \mathbb{N}(p)} D(m)_p^+$ comprising all elements $(x_m)_m$ with the property that for any m in $\mathbb{N}(p)$ and any prime ℓ one has

$$\mathrm{N}_m^{m\ell}(x_{m\ell}) = \begin{cases} x_m, & \text{if } \ell \text{ divides } m, \\ x_m^{1-\sigma_\ell}, & \text{otherwise.} \end{cases}$$

Now if f belongs to $\mathcal{F}^{\mathrm{d}}_{(p)}$, then for each n in $\mathbb{N}(p)$ the value of $f^{1+\tau}$ at ζ_n belongs to the (torsion-free) group $V(n)$ and hence can be regarded as an element of $V(n)_p$.

In view of Theorem 3.1, we can therefore use the assignment $f^{1+\tau} \leftrightarrow \{f(m)^{1+\tau}\}_m$ to identify $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}$ as a subgroup of $\mathcal{V}_p^{\mathrm{d}}$.

We can then consider the exact commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} & \longrightarrow & \mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} & \longrightarrow & \mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{d}}_{(p)} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \times p} & & \Big\downarrow{\scriptstyle \times p} & & \Big\downarrow{\scriptstyle \times p} & & \\
0 & \longrightarrow & \overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} & \longrightarrow & \mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} & \longrightarrow & \mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{d}}_{(p)} & \longrightarrow & 0
\end{array}$$

in which the rows are induced by the inclusions $\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} \subseteq \overline{\mathcal{F}}^{\mathrm{d}}_{(p)} \subseteq \mathcal{V}_p^{\mathrm{d}}$.

From Proposition 5.3(ii) and (iii) below we know that the second and third vertical arrows in this diagram are respectively bijective and injective and hence (by an application of the Snake Lemma) that the first vertical arrow is bijective.

This observation shows that the group $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$ is uniquely p-divisible, and hence proves Theorem 5.1(ii).

5.3.2. We recall that I_n denotes the annihilator in R_n^+ of the element ε_n and that this ideal is explicitly described in Lemma 2.4.

Before stating the next result we note that $\mathcal{V}_p^{\mathrm{d}}$ is naturally a module over the algebra

$$\Lambda_{(p)} := \varprojlim_{m\in\mathbb{N}(p)} R_{m,p}^+,$$

where the limit is taken with respect to the natural projection maps $R_n^+ \to R_m^+$ for each m in $\mathbb{N}(p)$ and each n in $\mathbb{N}(m)$.

Proposition 5.3.

(i) *The $\Lambda_{(p)}$-module $\mathcal{V}_p^{\mathrm{d}}$ is free of rank one with basis $\iota_p(\Phi^{1+\tau})$.*

(ii) *The quotient group $\mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$ is uniquely p-divisible.*

(iii) *The quotient group $\mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}$ has no element of order p.*

Proof. For each n in $\mathbb{N}(p)$ the map $R_{n,p}^+ \to D(n)_p^+$ that sends 1 to ε_n induces an isomorphism of $R_{n,p}$-modules $R_{n,p}^+/I_{n,p} \cong D(n)_p^+$. We therefore obtain a well-defined isomorphism of $\Lambda_{(p)}$-modules

$$\varepsilon : \prod_{n\in\mathbb{N}(p)} R_{n,p}^+/I_{n,p} \to \prod_{n\in\mathbb{N}(p)} D(n)_p^+$$

by defining $\varepsilon((r_n)_n)$ to be $(\varepsilon_n^{r_n})_n$.

Then the norm relations for the cyclotomic elements ε_n combine to imply that ε restricts to give an isomorphism

$$\mathcal{W}_p \cong \mathcal{V}_p^{\mathrm{d}}$$

where $\mathcal{W}_p$ denotes the $\Lambda_{(p)}$-submodule of $\prod_{n\in\mathbb{N}(p)} R_{n,p}^+/I_{n,p}$ comprising elements with the property that for every m in $\mathbb{N}(p)$ and every prime ℓ one has

($*_1$) $\pi_m^{m\ell}(r_{m\ell}) \equiv r_m$ modulo $I_{m,p}$ if ℓ divides m;

($*_2$) $\pi_m^{m\ell}((1-\sigma_\ell)\cdot r_{m\ell}) \equiv (1-\sigma_\ell)\cdot r_m$ modulo $I_{m,p}$ if ℓ is prime to m.

(Note that these congruence conditions are well-defined since for any m and any prime ℓ one has $\pi_m^{m\ell}(I_{m\ell}) \subseteq I_m$ if ℓ divides m and $(1-\sigma_\ell)\cdot\pi_m^{m\ell}(I_{m\ell}) \subseteq I_m$ if ℓ is prime to m.)

We write

$$\Delta_p : \Lambda_{(p)} \to \mathcal{W}_p$$

for the natural diagonal map.

Then for each r in $\Lambda_{(p)}$ and each n in $\mathbb{N}(p)$ one has $\varepsilon(\Delta_p(r))_n = \varepsilon_n^r = \iota_p(\Phi^{(1+\tau)})^r(n)$ and so $\varepsilon(\Delta_p(r)) = \iota_p(\Phi^{(1+\tau)})^r$. To prove claim (i) it is thus enough to show that Δ_p is bijective.

Injectivity of Δ_p follows directly from the first claim in Lemma 5.4 below. It is thus enough to show that each element $r = (r_m)_{m\in\mathbb{N}(p)}$ of $\mathcal{W}_p$ belongs to the image of Δ_p.

Now, for each such r and each m in $\mathbb{N}(p)$, the condition $(*_1)$ implies that the element $r_{mp^\infty} := (r_{mp^d})_{d\geq 0}$ belongs to $\varprojlim_d R^+_{mp^d,p}/I_{mp^d,p}$, where the transition morphisms are the natural projection maps, whilst Lemma 5.4 below implies that the natural projection map from $\Lambda_{(m,p)} := \varprojlim_d R^+_{mp^d,p}$ to $\varprojlim_d R^+_{mp^d,p}/I_{mp^d,p}$ is bijective.

For each m in $\mathbb{N}(p)$ and each multiple m' of m we therefore obtain a surjective composite homomorphism

$$\varpi_m^{m'} : \varprojlim_d R^+_{m'p^d,p}/I_{m'p^d,p} \cong \Lambda_{(m',p)} \to \Lambda_{(m,p)} \cong \varprojlim_d R^+_{mp^d,p}/I_{mp^d,p}$$

in which the arrow denotes the natural projection map.

We now assume that $m' = m\ell$ for a prime ℓ. If ℓ divides m, then $(*_1)$ implies directly that $\varpi_m^{m\ell}(r_{m\ell p^\infty}) = r_{mp^\infty}$. In addition, if ℓ does not divide m, then $(*_2)$ implies that the difference $\varpi_m^{m\ell}(r_{m\ell p^\infty}) - r_{mp^\infty}$ is annihilated by multiplication by $1-\sigma_\ell$ and hence, since $1-\sigma_\ell$ is a non-zero divisor in $\Lambda_{(m,p)}$, that $\varpi_m^{m\ell}(r_{m\ell p^\infty}) = r_{mp^\infty}$.

Since $\Lambda_{(p)}$ is equal to $\varprojlim_m \Lambda_{(m,p)}$, where m runs over $\mathbb{N}(p)$ and the transitions morphisms are the natural projection maps, this shows that r belongs to the image of Δ_p, as required to complete the proof of claim (i).

Turning to claim (ii) we note that the subgroup $\overline{\mathcal{F}}^{\rm c}_{(p)}$ of $\mathcal{V}_p^{\rm d}$ coincides with the image of the composite homomorphism

$$R \to \varprojlim_{m\in\mathbb{N}(p)} R^+_m \xrightarrow{\theta} \varprojlim_{m\in\mathbb{N}(p)} R^+_{m,p} = \Lambda_{(p)} \xrightarrow{\Delta_p} \mathcal{W}_p \xrightarrow{\varepsilon} \mathcal{V}_p^{\rm d}.$$

where the first map is the natural projection and θ is the natural inclusion.

In particular, since the first map in this composition is surjective and the last two are bijective, claim (ii) will follow if we can show that $\mathrm{cok}(\theta)$ is uniquely p-divisible.

To do this we note that for each m in $\mathbb{N}(p)$ and each m' in $\mathbb{N}(m)$ there exists a commutative diagram of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^+_{m'} & \xrightarrow{\subseteq} & R^+_{m',p} & \longrightarrow & (\mathbb{Z}_p/\mathbb{Z})\otimes_{\mathbb{Z}} R^+_{m'} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R^+_m & \xrightarrow{\subseteq} & R^+_{m,p} & \longrightarrow & (\mathbb{Z}_p/\mathbb{Z})\otimes_{\mathbb{Z}} R^+_m & \longrightarrow & 0 \end{array}$$

in which each vertical arrow is the natural projection map, and so is surjective.

Hence, by passing to the inverse limit over m of these sequences, we deduce that $\mathrm{cok}(\theta)$ is isomorphic to $\varprojlim_m(\mathbb{Z}_p/\mathbb{Z})\otimes_{\mathbb{Z}} R_m^+$ and hence is uniquely p-divisible since $\mathbb{Z}_p/\mathbb{Z}$ is.

To prove claim (iii) we note that $\mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}$ is a quotient of the uniquely p-divisible group $\mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$ and so has no element of order p if and only if the subgroup of elements of p-power order has bounded exponent.

To investigate this condition we write $\mathcal{U}$ for the subgroup of $\mathcal{F}^{\mathrm{d}}_{(p)}$ comprising all functions f with the property that for every n in $\mathbb{N}(p)$ the value $f(n)$ belongs to the (torsion-free) subgroup $V(n)$ of $E(n)'$.

It is then clear that $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}\subseteq\mathcal{U}$ and that an element $x=(x_n)_n$ of $\mathcal{V}_p^{\mathrm{d}}$ is equal to $(f(n))_n$ for some f in $\mathcal{U}$ if and only if one has $x_n\in V(n)$ for every n.

We now assume to be given an element c of $\mathcal{V}_p^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}$ of exact order p^t for some t and we lift c to an element $x=(x_n)_n$ of $\mathcal{V}_p^{\mathrm{d}}$.

Then, for each $n\in\mathbb{N}(p)$, we know that the element $x_n^{p^t}$ of $D(n)_p^+\subseteq V(n)_p$ belongs to $V(n)$. Since the quotient of $V(n)_p$ by $V(n)$ is uniquely p-divisible, it follows that x_n belongs to $V(n)$ and hence that $x=(f(n))_n$ for some f in $\mathcal{U}$.

Since $f^2=f^{1+\tau}$ belongs to $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}$ this in turn implies that the order p^t of c divides 2, as suffices to prove claim (iii). □

We end this section by proving a technical result about limits that was used above.

Lemma 5.4. *Fix m in $\mathbb{N}^*$ and a prime divisor p of m. For each natural number b write π'_b for the restriction of $\pi^{mp^{b+1}}_{mp^b}$ to $I_{mp^{b+1}}$ and $\pi'_{b,p}$ for the scalar extension $\mathbb{Z}_p\otimes_{\mathbb{Z}}\pi'_b$.*

Then the limit $\varprojlim_b(I_{mp^b,p},\pi'_{b,p})$ and first derived limit $\varprojlim^1_b(I_{mp^b,p},\pi'_{b,p})$ both vanish.

Proof. The vanishing of the derived limit $\varprojlim^1_b(I_{mp^b,p},\pi'_{b,p})$ follows directly from the Mittag-Leffler criterion and the fact that each module $I_{mp^b,p}$ is compact.

We note next that there exists a natural number b_0 such that all prime divisors of m have full decomposition group in $\mathrm{Gal}(\mathbb{Q}(mp^\infty)^+/\mathbb{Q}(mp^{b_0})^+)$.

Then to prove the vanishing of $\varprojlim_b(I_{mp^b,p},\pi'_{b,p})$ it is clearly enough to prove that for all $b\geq b_0$ one has

$$\mathrm{im}(\pi'_b)=p\cdot I_{mp^b} \tag{17}$$

and hence also $\mathrm{im}(\pi'_b)_p=p\cdot I_{mp^b,p}$. To prove this we fix $b\geq b_0$ and set $M:=mp^b$, $M_0:=mp^{b_0}$, $G:=G_M^+$ and $G_0:=G_{M_0}^+$.

If M is a power of p, then (17) follows immediately from the fact that I_M vanishes for all values of b by Example 2.5(i).

We therefore assume M is divisible by at least two primes. In this case the description of I_M given in Lemma 2.4 implies that, for any non-trivial homomorphism $\psi: G\to\mathbb{Q}^{c,\times}$, the idempotent e_ψ belongs to $\mathbb{Q}^c\otimes_{\mathbb{Z}} I_M$ if and only if there exists a prime ℓ that divides m and is such that its decomposition subgroup in G is contained in $\ker(\psi)$. This implies, in particular, that any such ψ factors through the projection $G\to G_0$.

Now any element x of I_M can be written uniquely as $\sum_\psi c_\psi\cdot e_\psi$ for suitable elements c_ψ of $\mathbb{Q}^c$, where ψ runs over all homomorphisms $G\to\mathbb{Q}^{c,\times}$.

In particular, if any term c_ψ in this sum is non-zero, then (since ε_M generates an R_M^+-module that is torsion-free) e_ψ must belong to $\mathbb{Q}^c \otimes_{\mathbb{Z}} I_M$ and hence ψ factors through the projection $G \to G_0$.

This observation implies that $x = hx$ for all elements h of $H := \mathrm{Gal}(\mathbb{Q}(M)^+/\mathbb{Q}(M_0)^+)$ and hence that I_M is equal to the set of elements of the form $x' \cdot \sum_{h\in H} h$ with $x' \in R_M^+$ such that $\pi^M_{M_0}(x') \in I_{M_0}$.

By using this description, one shows that the restriction of $\pi^M_{M_0}$ to I_M is both injective and has image $|H| \cdot I_{M_0}$ and then (17) follows easily from this fact. □

Remark 5.5. A closer analysis of the above argument shows that the inverse system of abelian groups $(I_{mp^b}, \pi'_b)_{b\in\mathbb{N}}$ is isomorphic to a direct sum of finitely many copies of the system $(X_b, \kappa_b)_{b\in\mathbb{N}}$ where $X_b := \mathbb{Z}$ for each b and each transition morphism κ_b is multiplication by p and this fact can be used to show that the derived limit $\varprojlim^1_b(I_{mp^b}, \pi'_b)$ is uniquely p-divisible. However, we make no use of this fact and so omit the details.

Remark 5.6. Proposition 5.3(i) also allows us to show that cyclotomic distributions satisfy the condition in Theorem 5.1(iii)(c) with $t = 1$ if p is odd and $t = 2$ if $p = 2$. To explain this, we fix r in R such that the distribution $f := \Phi^{(1+\tau)r}$ has $f(m) \in V(m)^{p^t}$ for all m in $\mathbb{N}(p)$, with t as specified above. Then for any n in $\mathbb{N}^* \setminus \mathbb{N}(p)$ the sequence $(f(np^a))_{a\in\mathbb{N}}$ is a p^t-th power in the limit $\mathcal{F}^{\mathrm{u}}(np)^\infty_p$ that occurs in Proposition 3.3 and hence also in the limit $C(np)^\infty_p$. The argument of [17, Th. 2.4] then allows one to deduce that each element $f(np^a)^2 = f(np^a)^{1+\tau}$ is a p^t-th power in the $R^+_{np^a,p}$-module generated by $\Phi^{1+\tau}(np^a)$. This then combines with the result of Proposition 5.3(i) to imply that the element of $\Lambda_{(p)}$ corresponding to $(1+\tau)2r$ is divisible by p^t, and hence in all cases that $(1+\tau)r$ belongs to pR. This in turn guarantees that $f(n)$ belongs to $V(n)^p$ for all n in $\mathbb{N}^*$, as required.

5.4. We now prove Theorem 5.1(iii).

To do this we first note that Theorem 4.1(iii) implies $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}}$ is uniquely p-divisible if and only if $\overline{\mathcal{F}}^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}$ is uniquely p-divisible. Then we use the fact that Theorem 5.1(i) gives rise to an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \overline{\mathcal{F}}^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}} \arrow[r, "\kappa_p"] \arrow[d, "\times p"'] & \overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} \arrow[r] \arrow[d, "\times p"'] & \mathrm{cok}(\kappa_p) \arrow[r] \arrow[d, "\times p"'] & 0 \\
0 \arrow[r] & \overline{\mathcal{F}}^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}} \arrow[r, "\kappa_p"] & \overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)} \arrow[r] & \mathrm{cok}(\kappa_p) \arrow[r] & 0
\end{tikzcd}$$

in which the central vertical arrow is bijective by Theorem 5.1(ii).

In particular, by applying the Snake Lemma to this diagram we deduce that $\overline{\mathcal{F}}^{\mathrm{d}}/\overline{\mathcal{F}}^{\mathrm{c}}$ is uniquely p-divisible if and only if the p-power torsion subgroup $\mathrm{cok}(\kappa_p)[p^\infty]$ of $\mathrm{cok}(\kappa_p)$ vanishes. Further, since $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$ is p-divisible, the group $\mathrm{cok}(\kappa_p)[p^\infty]$ is also p-divisible and so vanishes if and only if it has bounded exponent.

To prove equivalence of the stated conditions in Theorem 5.1(iii) it is thus enough to show that condition (c) implies $\mathrm{cok}(\kappa_p)[p^\infty]$ has bounded exponent.

To do this we assume the validity of condition (c), fix an element x of $\mathrm{cok}(\kappa_p)$ of exact order p^e and can further assume, without loss of generality, that e is strictly bigger than the integer t that occurs in condition (c).

We choose a map f in $\mathcal{F}^{\mathrm{d}}_{(p)}$ such that $f^{1+\tau}$ represents x and note that, by assumption, there exists a map f_e in $\mathcal{F}^{\mathrm{d}}$ with $\iota_p(f_e^{1+\tau}) = f^{(1+\tau)p^e}$.

By applying condition (c) to the map $f_e^{1+\tau}$ we can thus deduce that for every n in $\mathbb{N}^*$ there exists a (unique) element $h_{1,n}$ of the (torsion-free) group $V(n)$ with $f_e(n)^{1+\tau} = h_{1,n}^p$.

We then define $h_1 : \mu_\infty^* \to \mathbb{Q}^{c,\times}$ to be the unique $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$-equivariant map with $h_1(\zeta_n) = h_{1,n}$ for all n in $\mathbb{N}^*$.

Then $h_1^p = f_e^{1+\tau}$ and hence, as each group $V(n)$ is torsion-free, the function h_1 inherits the relation (1) from the map $f_e^{1+\tau}$ and so belongs to $\mathcal{F}^{\mathrm{d},+}$.

In a similar way, one has

$$\iota_p(h_1)^p = \iota_p(h_1^p) = \iota_p(f_e^{1+\tau}) = f^{(1+\tau)p^e}$$

and hence $\iota_p(h_1) = f^{(1+\tau)p^{e-1}}$.

Since, by assumption, $e-1 \geq t$ we can now repeat the above argument with $f_e^{1+\tau}$ replaced by h_1 in order to deduce the existence of a function h in $\mathcal{F}^{\mathrm{d},+}$ with $\iota_p(h) = f^{(1+\tau)p^{e-2}}$.

Then, as h is fixed by τ, the latter equality implies that $\iota_p(h^{1+\tau}) = \iota_p(h^2) = f^{(1+\tau)2p^{e-2}}$ and hence that the order of x divides $2p^{e-2}$.

This contradicts the assumption that the order of x is p^e, showing that the exponent of $\mathrm{cok}(\kappa_p)[p^\infty]$ must be bounded and hence completing the proof of Theorem 5.1(iii).

6. The proof of Theorem 1.2

In this section we prove Theorem 1.2 and then also justify the comments that follow the statement of this result in the Introduction.

6.1. To prove Theorem 1.2 we note at the outset that the results of Theorem 4.1(i) and (ii) combine to give a canonical exact commutative diagram of R-modules

$$\begin{tikzcd}
\widehat{\mathbb{Z}}(1) \arrow[r, hook] & \mathcal{F}^{\mathrm{d}}_{\mathrm{tf}} \arrow[r, two heads, "\mu"] & \overline{\mathcal{F}}^{\mathrm{d}} \\
\widehat{\mathbb{Z}}(1) \arrow[r, hook] \arrow[u, equal] & \mathcal{F}^{\mathrm{c}} \arrow[r, two heads, "\mu"] \arrow[u, hook] & \overline{\mathcal{F}}^{\mathrm{c}} \arrow[u, hook]
\end{tikzcd}$$

in which μ sends each f to $f^{1+\tau}$, the vertical arrows are the natural inclusions and, as in §5, we set $\overline{\mathcal{F}}^{\mathrm{d}} := (1+\tau)\mathcal{F}^{\mathrm{d}}$ and $\overline{\mathcal{F}}^{\mathrm{c}} := (1+\tau)\mathcal{F}^{\mathrm{c}}$.

To derive from this diagram the existence of a diagram as in Theorem 1.2 it is thus enough to describe a canonical injective homomorphism of R-modules

$$\kappa' : \overline{\mathcal{F}}^{\mathrm{d}} \to \widehat{R}(1+\tau) \tag{18}$$

with the property that $\kappa'(\overline{\mathcal{F}}^{\mathrm{c}})$ is equal to the image of the diagonal embedding of $R(1+\tau)$ in $\widehat{R}(1+\tau)$ (and one can then define the map κ in Theorem 1.2 to be the composite $\kappa' \circ \mu$).

To do this we use the canonical direct product decomposition of rings

$$\widehat{R} = \prod_p \widehat{R}^p.$$

Here the product is over all primes p and $\widehat{R}^p$ denotes the pro-p completion $\varprojlim_n R_{n,p}$ of R (so that in the inverse limit n runs over $\mathbb{N}$ and the transition maps are the standard projection maps).

Next we recall that the approach of §5 implies (via Proposition 5.3(i)) that for every f in $\overline{\mathcal{F}}^{\rm d}$ there exists a unique element $r_{f,p}$ of $\widehat{R}^p(1+\tau)$ with the property that for each n in $\mathbb{N}(p)$ one has $f(n) = \Phi(n)^{r_{f,p}}$ in $V(n)_p$.

We can therefore define a map as in (18) by specifying that for each f in $\overline{\mathcal{F}}^{\rm d}$ one has $\kappa'(f) = (r_{f,p})_p$.

With this definition, it is clear that κ' is a homomorphism of R-modules, that κ' is injective and also, since $\overline{\mathcal{F}}^{\rm c} = R(1+\tau)\cdot\Phi$, that $\kappa'(\overline{\mathcal{F}}^{\rm c}) = R(1+\tau)$.

This completes the proof of Theorem 1.2.

Remark 6.1. A closer analysis of the above construction gives an explicit description of the map $\kappa = \kappa'\circ\mu$ that occurs in Theorem 1.2. To explain this we fix f in $\mathcal{F}^{\rm d}$ and m in $\mathbb{N}^*$. Then for every prime p the argument in §5 shows that for each n in $\mathbb{N}$ there exists an element $a_n = a_{f,m,n,p}$ of $R^+_{mp^n,p}$ with $f^{1+\tau}(mp^n) = \varepsilon_{mp^n}^{a_n}$ in $V(mp^n)_p$, that the sequence $(\pi_m^{mp^n}(a_n))_n$ is convergent in $R^+_{m,p}$, that the limit $a_{f,m,p} := \lim_{n\to\infty}\pi_m^{mp^n}(a_n)$ is independent of the choice of elements a_n and that the tuple $(a_{f,m,p})_m$ belongs to $\varprojlim_m R^+_{m,p}$. Writing $a_{f,p}$ for the pre-image of $(a_{f,m,p})_m$ under the isomorphism of $\widehat{R}^p$-modules $\widehat{R}^p(1+\tau)\to\varprojlim_m R^+_{m,p}$ that sends $1+\tau$ to 1, one then has $\kappa(f) = (a_{f,p})_p$.

Remark 6.2. The exact sequence of R-modules given by the lower row of the diagram in Theorem 1.2 splits after inverting 2 since the map sending $1+\tau$ to $\Phi^{(1+\tau)/2}$ is a section to the restriction of $\mathbb{Z}[\frac{1}{2}]\otimes_{\mathbb{Z}}\kappa$ to $\mathbb{Z}[\frac{1}{2}]\otimes_{\mathbb{Z}}\mathcal{F}^{\rm c}$ in this case. However, the sequence does not itself split, even as a sequence of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-modules, since if this was true there would exist f in $\mathcal{F}^{\rm c}$ with $f = f^\tau$ and such that $\kappa(f) = 1+\tau$. This would in turn imply the existence of an element r of R with both $\Phi^{(1-\tau)r} = 1$ and $(1+\tau)r = 1+\tau$. The second equality here implies $r = 1 - r'(1-\tau)$ for some r' in R and then the first equality implies $\Phi^{1-\tau} = \Phi^{2r'(1-\tau)}$. But this cannot be true since, for example, $\Phi^{1-\tau}(4) = -\zeta_4$ is not a square in $\mathbb{Q}(4)$.

Remark 6.3. In this remark we set $\Gamma := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and note that for any Γ-module M the Tate cohomology group $\hat{H}^0(\Gamma, M) := M^{\tau=1}/(1+\tau)M$ is a vector space over the field of two elements $\mathbb{F}_2$. Then, since the module of Coleman distributions $\mathcal{D}$ is the torsion subgroup of $\mathcal{F}^{\rm d}$ (cf. Remark 4.5), there is a natural isomorphism

$$\hat{H}^0(\Gamma, \mathcal{F}^{\rm d}_{\rm tf}) \cong \frac{\{f\in\mathcal{F}^{\rm d} : f^{\tau-1}\in\mathcal{D}\}}{\mathcal{D} + (1+\tau)\mathcal{F}^{\rm d}}$$

and hence also an exact sequence of $\mathbb{F}_2$-vector spaces

$$0\to\mathcal{D}\to\hat{H}^0(\Gamma,\mathcal{F}^{\rm d})\to\hat{H}^0(\Gamma,\mathcal{F}^{\rm d}_{\rm tf})\to\mathcal{D}\cap(1-\tau)\mathcal{F}^{\rm d}\to 0. \tag{19}$$

Here the second map is induced by the inclusion $\mathcal{D} \subset \mathcal{F}^{\mathrm{d},\tau=1}$ (and so is injective since $\mathcal{D}\cap(1+\tau)\mathcal{F}^{\mathrm{d}} = 0$), the third is obvious and the fourth is induced by sending each distribution f to $f^{1-\tau}$. In particular, since $\mathcal{D}$ is a vector space over $\mathbb{F}_2$ of uncountably infinite dimension, this shows that the group $\hat{H}^0(\Gamma, \mathcal{F}^{\mathrm{d}})$ is large. To be more explicit we assume Coleman's Conjecture to be valid so that $\mathcal{F}^{\mathrm{d}} = \mathcal{D} + \mathcal{F}^{\mathrm{c}}$. Then $\mathcal{D} \cap (1-\tau)\mathcal{F}^{\mathrm{d}}$ is equal to $\mathcal{D} \cap (1-\tau)\mathcal{F}^{\mathrm{c}}$ and so vanishes, and $\hat{H}^0(\Gamma, \mathcal{F}^{\mathrm{d}}_{\mathrm{tf}})$ identifies with $\hat{H}^0(\Gamma, \mathcal{F}^{\mathrm{c}})$. In addition, by considering Tate cohomology of the (exact) lower row of the diagram in Theorem 1.2, one finds that the results of Theorem 4.1(i) and (ii) combine to give a natural exact sequence

$$0 \to \hat{H}^0(\Gamma, \mathcal{F}^{\mathrm{c}}) \to \mathbb{F}_2 \otimes_{\mathbb{Z}} R(1+\tau) \to \mathbb{F}_2 \to 0.$$

This sequence then combines with (19) to give an exact sequence of the form

$$0 \to \mathcal{D} \to \hat{H}^0(\Gamma, \mathcal{F}^{\mathrm{d}}) \to \mathbb{F}_2 \otimes_{\mathbb{Z}} R(1+\tau) \to \mathbb{F}_2 \to 0.$$

Remark 6.4. For each prime p write $\mathcal{F}^{\dagger}_{(p)}$ for the R-submodule of $\mathcal{F}$ comprising functions whose image under the restriction map ι_p belongs to $\mathcal{F}^{\mathrm{d}}_{(p)}$. Then $\mathcal{F}^{\mathrm{d}}$ is the intersection of $\mathcal{F}^{\dagger}_{(p)}$ over all p and so there is an inclusion of $\overline{\mathcal{F}}^{\mathrm{d}} = (1+\tau)\mathcal{F}^{\mathrm{d}}$ into $\bigcap_p (1+\tau)(\mathcal{F}^{\dagger}_{(p)})$ whose cokernel is annihilated by 2. Taking account of the isomorphism in Theorem 4.1(iii) one therefore obtains inclusions

$$2 \cdot \bigcap_p \frac{(1+\tau)(\mathcal{F}^{\dagger}_{(p)})}{\overline{\mathcal{F}}^{\mathrm{c}}} \subseteq \frac{\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}}{\mathcal{F}^{\mathrm{c}}} \subseteq \bigcap_p \frac{(1+\tau)(\mathcal{F}^{\dagger}_{(p)})}{\overline{\mathcal{F}}^{\mathrm{c}}}$$

in which both intersections run over all p. For each p there is also a natural exact sequence

$$0 \to (1+\tau)\mathcal{F} \cap \ker(\iota_p) \to \frac{(1+\tau)(\mathcal{F}^{\dagger}_{(p)})}{\overline{\mathcal{F}}^{\mathrm{c}}} \to \frac{\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}}{\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}} \to 0,$$

in which the third map is induced by ι_p and exactness follows from the fact $\overline{\mathcal{F}}^{\mathrm{c}}$ is disjoint from $\ker(\iota_p)$. In particular, since Lemma 2.1 implies $\overline{\mathcal{F}}^{\mathrm{d}}$ is also disjoint from $\ker(\iota_p)$, this sequence induces an identification of $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}}$ with a submodule of $\overline{\mathcal{F}}^{\mathrm{d}}_{(p)}/\overline{\mathcal{F}}^{\mathrm{c}}_{(p)}$. Finally we recall that, by Theorem 5.1(ii), the latter group is uniquely p-divisible.

Remark 6.5. If Coleman's Conjecture is valid, and f in $\mathcal{F}^{\mathrm{d}}$ is not torsion-valued, then the lower row of the diagram in Theorem 1.2 implies that the set of primes $\{\ell : \kappa(f) \in \ell \cdot \widehat{R}(1+\tau)\}$ is finite. The following result provides evidence that this is a reasonable expectation.

Lemma 6.6. *If f in $\mathcal{F}^{\mathrm{d}}$ is not torsion-valued, then the set of primes $\{\ell : \kappa(f) \in \ell \cdot \widehat{R}(1+\tau)\}$ has Dirichlet density zero.*

Proof. Set $f' := f^{1+\tau}$. Then, since f is not torsion-valued, Lemma 4.3 implies there exists m in $\mathbb{N}^*$ such that $f'(m) \neq 1$. By using Lemma 2.1 we can also assume that m is divisible by an odd prime p.

Then there exists an n_0 in $\mathbb{N}$ such that for all $n > n_0$ one has $f'(mp^n) \notin \mathbb{Q}(mp^{n-1})^+$. Indeed, if this is not true, then the norm compatibility of the elements $\{f'(mp^a)\}_{a \geq 0}$ implies $f'(m) \in V(m)^{p^t}$ for arbitrarily large integers t and, since $V(m)$ is torsion-free, this contradicts the assumption that $f'(m) \neq 1$.

Fix $n > n_0$ and an element σ of $G^+_{mp^n}$ and write $\mathcal{P}_\sigma$ for the set of primes q that do not divide m and are such that the restriction of σ_q to $\mathbb{Q}(mp^n)^+$ is equal to σ.

Then for any q in the intersection of $\mathcal{P}_\sigma$ with $\mathcal{P}_f := \{\ell : \kappa(f) \in \ell \cdot \widehat{R}(1+\tau)\}$, the distribution relation

$$f'(mp^n)^{1-\sigma} = f'(mp^n)^{1-\sigma_q} = \mathrm{N}^{mp^nq}_{mp^n}(f'(mp^nq)) = \mathrm{N}^{mp^nq}_{mp^n}((\varepsilon_{mp^nq})^{\kappa(f)_q})$$

in $V(mp^n)_q$ implies that $f'(mp^n)^{1-\sigma}$ belongs to $V(mp^n)^q$.

Thus, if σ is such that $\mathcal{P}_\sigma \cap \mathcal{P}_f$ is infinite, then $f'(mp^n)^{1-\sigma} = 1$. In any such case, the fact that $f'(mp^n) \notin \mathbb{Q}(mp^{n-1})^+$ therefore implies that the subgroup generated by σ must be disjoint from the cyclic subgroup $\mathrm{Gal}(\mathbb{Q}(mp^n)^+/\mathbb{Q}(m'p)^+)$ of $G^+_{mp^n}$, where we write m' for the maximal divisor of m that is prime to p.

In particular, if the p-exponent of $G^+_{m'p}$ is p^{n_1}, then for any $n > n_0 + n_1$ the maximal power of p that divides the order of σ is at most p^{n_1} whilst the maximal power of p that divides the exponent of $G^+_{mp^n}$ is at least p^{n-1}.

This implies that $\#\{\sigma \in G^+_{mp^n} : \mathcal{P}_\sigma \cap \mathcal{P}_f \text{ is infinite }\}$ is at most $\#G^+_{mp^n}/p^{n-1-n_1}$ and hence, by the Tchebotarev Density Theorem, that the density of $\mathcal{P}_f$ is at most p^{n_1+1-n}.

The claimed result therefore follows from the fact that p^{n_1+1-n} tends to 0 as n tends to infinity. □

6.2. In this section we derive from Theorem 1.2 an explicit criterion for a distribution to be cyclotomic. This criterion is reminiscent of the archimedean 'boundedness' criterion that Coleman uses in [3] to characterise cyclotomic units in p-power conductor abelian fields.

To do this we recall that, by the argument in §5, for each function f in $\mathcal{F}^{\mathrm{d}}$ and each m and n in $\mathbb{N}$ there exists a (non-unique) element $a_{m,n}(f)$ in $R^+_{mp^n,p}$ such that in $V(mp^n)_p$ one has

$$f^{1+\tau}(mp^n) = (\varepsilon_{mp^n})^{a_{m,n}(f)}. \tag{20}$$

For any natural number k with $k \le n$ and any element x of $R^+_{mp^n,p}$ we write $|x|_k$ for the unique integer in $\{a : 0 \le a < p^{n-k}\}$ that is equal to the coefficient of the trivial element of G^+_m in the standard representation of the image of x under the composite map

$$R^+_{mp^n,p} \to R^+_{m,p} \to \mathbb{Z}_p/(p^{n-k}) \otimes_{\mathbb{Z}_p} R^+_{m,p} = \mathbb{Z}/(p^{n-k}) \otimes_{\mathbb{Z}} R^+_m,$$

where the first map is induced by $\pi^{mp^n}_m$ and the second is the natural reduction map.

We shall then say that a given subset of $\mathcal{F}^{\mathrm{d}}$ is 'p-bounded' if for each of its elements f, each m in $\mathbb{N}(p)$ and any sufficiently large k at least one of the sets $\{|a_{m,n}(f)|_k\}_{n>k}$ and $\{|-a_{m,n}(f)|_k\}_{n>k}$ is bounded. (See Remark 6.8 below).

Theorem 6.7. *Fix f in $\mathcal{F}^{\mathrm{d}}$. Then f is cyclotomic if and only if for any, and therefore for every, prime p the set of distributions $\{f^\sigma : \sigma \in \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})\}$ is p-bounded.*

Proof. It is enough to fix a prime p and show that f is cyclotomic if and only if the set $\{f^\sigma : \sigma \in \mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})\}$ is p-bounded.

At the outset, we note that the diagram in Theorem 1.2 implies directly that f is cyclotomic if and only if $f^{1+\tau}$ belongs to $(1+\tau)\mathcal{F}^{\mathrm{c}}$.

Hence, in view of Theorem 5.1(i), one knows that f is cyclotomic if and only if the restriction $\iota_p(f^{1+\tau})$ of $f^{1+\tau}$ belongs to $(1+\tau)\mathcal{F}^{\mathrm{c}}_{(p)}$.

Now the definition (given in §6.1) of the map κ in Theorem 1.2 implies that the projection $\kappa(f)_p$ of $\kappa(f)$ to $\widehat{R}^p(1+\tau)$ is the unique element with the property that for each m in $\mathbb{N}(p)$ one has $f^{1+\tau}(m) = \Phi(m)^{\kappa(f)_p}$ in $V(m)_p$. It follows that f is cyclotomic if and only if $\kappa(f)_p$ belongs to $R(1+\tau)$.

We next recall from Remark 6.1 that, for any choice of elements $a_{m,b}(f)$ as in (20), the sequence $(\pi_m^{mp^b}(a_{m,b}(f)))_{b\in\mathbb{N}}$ is convergent in $R^+_{m,p}$ and that $\kappa(f)_p$ is the element of the limit $\widehat{R}^p(1+\tau) \cong \varprojlim_m R^+_{m,p}$ that corresponds to $(\lim_{b\to\infty}\pi_m^{mp^b}(a_{m,b}(f)))_m$.

This implies that $\kappa(f)_p$ belongs to $R(1+\tau)$ if and only if for every m in $\mathbb{N}(p)$ the limit $\lim_{b\to\infty}\pi_m^{mp^b}(a_{m,b}(f))$ belongs to R^+_m.

Now, if for each b in $\mathbb{N}$ and g in G^+_m, we define p-adic integers $c_{m,b,g}(f)$ by the equality

$$\pi_m^{mp^b}(a_{m,b}(f)) = \sum_{g\in G^+_m} c_{m,b,g}(f)\cdot g,$$

then each sequence $(c_{m,b,g}(f))_b$ is convergent in $\mathbb{Z}_p$ and one has

$$\lim_{b\to\infty}\pi_m^{mp^b}(a_{m,b}(f)) = \sum_{g\in G^+_m}(\lim_{b\to\infty} c_{m,b,g}(f))\cdot g.$$

In addition, for any element g of G^+_m and any element σ of $\mathrm{Gal}(\mathbb{Q}^c/\mathbb{Q})$ that restricts on $\mathbb{Q}(m)^+$ to give g^{-1} one can take the elements $a_{m,b}(f^\sigma)$ in (20) to be $\sigma\cdot a_{m,b}(f)$ and in this way compute that $c_{m,b,g}(f) = c_{m,b,e}(f^\sigma)$ where e is the identity element of G^+_m.

This observation reduces us to showing that for every m in $\mathbb{N}(p)$ and every f in $\mathcal{F}^{\mathrm{d}}$ the limit $c := \lim_{b\to\infty} c_{m,b,e}(f)$ belongs to $\mathbb{Z}$ if and only if for any sufficiently large integer k at least one of the sets $\{|a_{m,n}(f)|_k\}_{n>k}$ and $\{|-a_{m,n}(f)|_k\}_{n>k}$ is bounded.

If, firstly, c is a non-negative integer, then, since c is the coefficient of e in the limit $\lim_{n\to\infty}\pi_m^{mp^n}(a_{m,n}(f))$ one must have $|a_{m,n}(f)|_k = c$ for all sufficiently large n and so the set $\{|a_{m,n}(f)|_k\}_{n>k}$ is indeed bounded.

Similarly, if c is a negative integer, then $|-a_{m,n}(f)|_k$ must be equal to $-c$ for all sufficiently large n and so $\{|-a_{m,n}(f)|_k\}_{n>k}$ is bounded.

To prove the converse we fix k such that either $\{|a_{m,n}(f)|_k\}_{n>k}$ or $\{|-a_{m,n}(f)|_k\}_{n>k}$ is bounded and choose a strictly increasing sequence of natural numbers $(n_i)_i$ with $n_i > k$ and $c_{m,n_i,e}(f) \equiv c \pmod{p^{n_i-k}}$ for each i.

Then, with $c(i)$ denoting the unique integer in $\{a : 0 \le a < p^{n_i-k}\}$ with $c(i) \equiv c_{m,n_i,e}(f) \pmod{p^{n_i-k}}$, one finds that the element $(c(i))_i$ belongs to $\mathbb{Z}_p = \varprojlim_i \mathbb{Z}/(p^{n_i-k})$ and is equal to c.

Now, if $\{|a_{m,n}(f)|_k\}_{n>k}$ is bounded, then the definition of $|a_{m,n}(f)|_k$ ensures that the increasing sequence $(c(i))_i$ is eventually constant. This implies that c is equal to $c(i)$ for any large enough value of i and so is a non-negative integer.

Similarly, if $\{|-a_{m,n}(f)|\}_{n>k}$ is bounded, then we can repeat the above argument with each term $a_{m,n}(f)$ replaced by $-a_{m,n}(f)$ to deduce that $-c$ is a non-negative integer, as required to complete the proof. $\square$

Remark 6.8. It is easily seen that the condition of being p-bounded is independent of the precise choice of elements $a_{m,n}(f)$ that occur in the equality (20). To be specific, if one fixes m and considers any other choice $\{a'_{m,n}(f)\}_n$ of such elements, then for each n one has $a_{m,n}(f) - a'_{m,n}(f) \in I_{mp^n,p}$. In particular, if one chooses k to be greater than the integer b_0 that occurs in the proof of Lemma 5.4, then the latter argument shows that for every $n > k$ one has $\pi_m^{mp^n}(a_{m,n}(f) - a'_{m,n}(f)) \in p^{n-k} \cdot R^+_{m,p}$ and hence that $|a_{m,n}(f)|_k = |a'_{m,n}(f)|_k$.

Remark 6.9. For the norm compatible family discussed in Lemma 2.10(i) it can be shown that there is no natural number k for which either of the sets $\{|\Pi_n|_k\}_{n>k}$ or $\{|-\Pi_n|_k\}_{n>k}$ is bounded, where each Π_n is regarded as an element of $R^+_{qp^n}$. In view of Theorem 6.7, Coleman's Conjecture therefore predicts that no such family can arise as the restriction of a distribution. However, aside from the special case considered in Lemma 2.10(ii), we have not yet been able to verify this prediction.

7. Divisible distributions

We say that a distribution is 'p-divisible' for some prime p, respectively is 'divisible', if its image in $\mathcal{F}^{\rm d}_{\rm tf}/\mathcal{F}^{\rm c}$ is p-divisible, respectively is divisible, and we write $\mathcal{F}^{\rm d}_{\rm pdiv}$ and $\mathcal{F}^{\rm d}_{\rm div}$ for the R-submodules of $\mathcal{F}^{\rm d}$ comprising all such distributions.

Irrespective of the validity, or otherwise, of Coleman's Conjecture, such distributions are closely related to circular distributions and share many of the same properties (see Proposition 7.2 below).

In Theorem 5.1(iii) we described an explicit criterion for *every* distribution to be p-divisible.

In this section we explain how the map κ in Theorem 1.2 also leads to an explicit criterion for a given distribution to be either p-divisible or divisible.

7.1. For each f in $\mathcal{F}^{\rm d}$ and each prime p we write $\kappa(f)_p$ for the image of $\kappa(f)$ under the natural projection $\widehat{R}(1+\tau) \to \widehat{R}^p(1+\tau)$.

Proposition 7.1. *For each distribution f in $\mathcal{F}^{\rm d}$ the following claims are valid.*

(i) *f is p-divisible if and only if for each m in $\mathbb{N}^*$ one has*

$$f(m)^{1+\tau} = \Phi(m)^{\kappa(f)_p}$$

in $V(m)_p$.

(ii) *f is divisible if and only if for each m in $\mathbb{N}^*$ one has*

$$f(m)^{1+\tau} = \Phi(m)^{\kappa(f)}$$

in $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} V(m)$.

Proof. To prove claim (i) we assume first that f is p-divisible. Then for each natural number n there exists an element $s(n)'$ of R and functions δ_n in $\mathcal{D} = \mathcal{F}^{\rm d}_{\rm tor}$ and f_n in $\mathcal{F}^{\rm d}$ such that

$$f \cdot \Phi^{-s(n)'} = \delta_n \cdot f_n^{p^n}.$$

Setting $s(n) := (1+\tau)s(n)'$, this fact implies that $\kappa(f)-s(n) = \kappa(f\cdot\Phi^{-s(n)'}) = p^n\cdot\kappa(f_n)$. For each m in $\mathbb{N}^*$ this in turn gives equalities in $V(m)_p$ of the form

$$\begin{aligned} f(m)^{1+\tau} =& \Phi(m)^{s(n)_p}\cdot f_n(m)^{p^n(1+\tau)} \\ =& \Phi(m)^{\kappa(f)_p}\cdot\Phi(m)^{-\kappa(f)_p+s(n)_p}\cdot f_n(m)^{p^n(1+\tau)} \\ =& \Phi(m)^{\kappa(f)_p}\cdot(\Phi(m)^{-\kappa(f_n)_p}\cdot f_n(m)^{(1+\tau)})^{p^n} \end{aligned}$$

It follows that $f(m)^{1+\tau}\cdot\Phi(m)^{-\kappa(f)_p}$ belongs to $V(m)_p^{p^n}$ for all n and hence that $f(m)^{1+\tau} = \Phi(m)^{\kappa(f)_p}$, as claimed.

To prove the converse we assume that $f(m)^{1+\tau} = \Phi(m)^{\kappa(f)_p}$ in $V(m)_p$ for all m in $\mathbb{N}^*$. For each n in $\mathbb{N}$ we can then fix an $r(n)$ in $R(1+\tau)$ such that $\kappa(f) - r(n) = p^n\cdot s(n)$ for some $s(n)$ in $\widehat{R}(1+\tau)$.

For each m in $\mathbb{N}^*$ one therefore has

$$f(m)^{1+\tau} = \Phi(m)^{\kappa(f)_p} = \Phi(m)^{r(n)}\cdot\Phi(m)^{p^n\cdot s(n)_p}$$

in $V(m)_p$ and hence $(f^{1+\tau}\Phi^{-r(n)})(m)\in V(m)\cap(V(m)_p)^{p^n}$. Since the group $V(m)_p/V(m)$ is uniquely p-divisible, it follows that $(f^{1+\tau}\Phi^{-r(n)})(m)$ belongs to $V(m)^{p^n}$ for all m.

In particular, since each group $V(m)$ is torsion-free, there exists a unique element $h_{n,m}$ of $V(m)$ with $(f^{1+\tau}\Phi^{-r(n)})(m) = (h_{n,m})^{p^n}$ and the unique map h_n in $\mathcal{F}$ with $h_n(m) := h_{n,m}$ for all m in $\mathbb{N}^*$ inherits the property of being a distribution from $f^{1+\tau}\Phi^{-r(n)}$.

But then the equality of functions

$$(f^{1+\tau}\Phi^{-r(n)})^2 = (f^{1+\tau}\Phi^{-r(n)})^{1+\tau} = (h_n^{1+\tau})^{p^n} \tag{21}$$

implies that the image of $f^{2(1+\tau)}$ is p-divisible in $(1+\tau)\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/(1+\tau)\mathcal{F}^{\mathrm{c}}$ and hence, via the isomorphism in Theorem 4.1(iii), that f^2 is p-divisible. If p is odd, then this directly implies that f is p-divisible.

On the other hand, if $p = 2$, then since all the functions in (21) are valued in torsion-free groups, this equality implies that $f^{1+\tau}\Phi^{-r(n)} = (h_n^{1+\tau})^{2^{n-1}}$ and, by the same argument as above, this implies that f is 2-divisible.

Claim (ii) follows directly from claim (i) and the obvious fact that f is divisible if and only if it is p-divisible for all primes p. □

7.2. In this final section we verify that divisible distributions have many of the same properties as do cyclotomic distributions, thus justifying an observation made in the Introduction.

We write $\mathcal{F}^{\mathrm{sd}}_{\mathrm{div}}$ for the submodule of $\mathcal{F}^{\mathrm{sd}}$ comprising all strict distributions whose image in $\mathcal{F}^{\mathrm{d}}_{\mathrm{tf}}/\mathcal{F}^{\mathrm{c}}$ is divisible.

We shall also say that two subsets $\mathcal{F}_1$ and $\mathcal{F}_2$ of $\mathcal{F}$ 'have the same values' if for each n in $\mathbb{N}^*$ the sets $\{f(n) : f\in\mathcal{F}_1\}$ and $\{f(n) : f\in\mathcal{F}_2\}$ generate the same R-module.

Proposition 7.2.

(i) *One has* $\mathcal{F}^{\mathrm{d}}_{\mathrm{div}} = \mathcal{D} + \mathcal{F}^{\mathrm{sd}}_{\mathrm{div}}$.

(ii) *The groups* $\mathcal{F}^{\mathrm{c}}$, $\mathcal{F}^{\mathrm{sd}}_{\mathrm{div}}$ *and* $\mathcal{F}^{\mathrm{d}}_{\mathrm{div}}$ *have the same values.*

(iii) *If f is any element of $\mathcal{F}^{\rm d}_{\rm div}$, then there exist precisely two finite products δ of functions of the form δ_Π, for suitable sets of odd primes Π, for which, at each n in $\mathbb{N}^*$, each prime ℓ that does not divide n, each ε in μ_ℓ and each ζ in μ_n^* one has*

$$\delta(\varepsilon\cdot\zeta)\cdot f(\varepsilon\cdot\zeta)\equiv\delta(\zeta)\cdot f(\zeta)\quad \textit{modulo all primes above } \ell. \tag{22}$$

(iv) *If f is any element of $\mathcal{F}^{\rm d}_{\rm div}$, then there exists an integer v that depends only on f and is such that for all primes p and all natural numbers n, the valuation of $f(p^n)$ at the unique prime of $\mathbb{Q}(p^n)$ above p is equal to v.*

(v) *If f is any element of $\mathcal{F}^{\rm d}_{\rm div}$, then for any odd prime p there exists an element of $\mathcal{F}^{\rm c}$ that (may depend on p and) agrees with f when evaluated at any root of unity of p-power order.*

Proof. The key point is to note is that if f belongs to $\mathcal{F}^{\rm d}_{\rm div}$, then for each natural number t there exist maps $\delta_{f,t}$ in $\mathcal{F}^{\rm d}_{\rm tor}=\mathcal{D}$ (cf. Remark 4.5), f_t in $\mathcal{F}^{\rm d}$ and $f_t^{\rm c}$ in $\mathcal{F}^{\rm c}$ such that

$$f=\delta_{f,t}\cdot f_t^{\rm c}\cdot (f_t)^t. \tag{23}$$

To prove claim (i) we note that f belongs to $\mathcal{F}^{\rm sd}$ if and only if for all natural numbers n, all primes ℓ that are coprime to n, all ε in μ_ℓ and all ζ in μ_n^* it satisfies the congruence (2).

To check this we write $t_{n,\ell}$ for any choice of n and ℓ as above for the product of the orders of the multiplicative groups of the residue fields of $\mathbb{Q}(n)$ at each prime above ℓ.

Then, for any given value of n and ℓ, the congruence (2) is clearly satisfied by the $t_{n,\ell}$-th power of any map in $\mathcal{F}^{\rm d}$. We also know that this congruence is satisfied by any map in $\mathcal{F}^{\rm c}$ and that the square of any map in $\mathcal{D}$ is trivial.

In particular, if for any given n and ℓ we combine these facts with the equality (23) with $t=t_{n,\ell}$, we find that f^2 satisfies the congruence (2) for this choice of n and ℓ.

Thus, since n and ℓ are arbitrary, we deduce that the square of any map f in $\mathcal{F}^{\rm d}_{\rm div}$ belongs to $\mathcal{F}^{\rm sd}$, and hence also to $\mathcal{F}^{\rm sd}_{\rm div}$.

This shows that the quotient of $\mathcal{F}^{\rm d}_{\rm div}$ by $X:=\mathcal{D}+\mathcal{F}^{\rm sd}_{\rm div}$ has exponent dividing 2. On the other hand, since $\mathcal{F}^{\rm c}\subseteq X$, the group $\mathcal{F}^{\rm d}_{\rm div}/X$ is isomorphic to a quotient of the image of $\mathcal{F}^{\rm d}_{\rm div}$ in $\mathcal{F}^{\rm d}_{\rm tf}/\mathcal{F}^{\rm c}$ and so is divisible. It follows that $\mathcal{F}^{\rm d}_{\rm div}/X$ is trivial, and hence that claim (i) is valid.

Noting $\mathcal{F}^{\rm c}\subseteq\mathcal{F}^{\rm sd}_{\rm div}\subseteq\mathcal{F}^{\rm d}_{\rm div}$, to prove claim (ii) it suffices to show that for any f in $\mathcal{F}^{\rm d}_{\rm div}$ and any n in $\mathbb{N}^*$ the element $f(n)$ of $E(n)'$ belongs to the R_n-submodule generated by $1-\zeta_n$.

By the same argument as in §3.4, it is thus enough to show that the image $f(n)'$ of $f(n)$ in $E(n)'_{\rm tf}$ belongs to the group $C(n)'_{\rm tf}$, where the group of cyclotomic numbers $C'(n)$ is as defined in §3.2.3.

But for any t in $\mathbb{N}$ the decomposition (23) implies that $f(n)'$ belongs to $C'(n)_{\rm tf}\cdot(E(n)'_{\rm tf})^t$. Since t is arbitrary, this in turn implies that $f(n)'$ belongs to $C'(n)_{\rm tf}$, as required to prove claim (ii).

Claim (i) implies that for any f in $\mathcal{F}^{\rm d}_{\rm div}$ there exists a map δ in $\mathcal{D}$ such that $\delta\cdot f$ belongs to $\mathcal{F}^{\rm sd}$ or, equivalently, such that the congruences (2) are satisfied.

In addition, if δ' is any other map in $\mathcal{D}$ with this property, then $\delta^{-1}\delta'=(\delta\cdot f)^{-1}(\delta'\cdot f)$ belongs to $\mathcal{D}\cap\mathcal{F}^{\rm sd}$ and so is either trivial or equal to the map $\delta_{\rm odd}$ described in the Introduction. This proves claim (iii).

For each prime p and each natural number m we write val_{p^m} for the standard valuation of $\mathbb{Q}(p^m)$ at the unique prime ideal above p.

We further note that, for any r in R, the valuation $\mathrm{val}_{p^m}((1-\zeta_{p^m})^r)$ is equal to the image of r under the natural projection map $R \to \mathbb{Z}$ and so is independent of both p and m. It is also clear that for any δ in $\mathcal{D}$ one has $\mathrm{val}_{p^m}(\delta(p^m)) = 0$.

For any f in $\mathcal{F}^{\mathrm{d}}_{\mathrm{div}}$, these observations combine with (23) to imply, for any given primes p and q, and any given natural numbers t, m and n, that there are congruences modulo t of the form

$$\mathrm{val}_{p^m}(f(p^m)) \equiv \mathrm{val}_{p^m}(f^{\mathrm{c}}_t(p^m)) = \mathrm{val}_{q^n}(f^{\mathrm{c}}_t(q^n)) \equiv \mathrm{val}_{q^n}(f(q^n)).$$

Since t is arbitrary, this implies $\mathrm{val}_{p^m}(f(p^m)) = \mathrm{val}_{q^n}(f(q^n))$ for all p, q, m and n and so proves claim (iv).

To prove claim (v) we fix an odd prime p and write $\mu^*_{p^\infty}$ for the set of non-trivial roots of unity of p-power order.

We recall that the result of [18, Th. B] implies the existence of a natural number m that depends only on p and is such that for any f in $\mathcal{F}^{\mathrm{d}}$ there exists a map $g_{f,m}$ in $\mathcal{F}^{\mathrm{c}}$ which agrees with f^m on $\mu^*_{p^\infty}$.

Next we note that if δ is any element of $\mathcal{D}$, then there exists an integer a (depending on δ) such that $\delta(p^m) = (-1)^a$ for every m.

This shows that δ agrees on $\mu^*_{p^\infty}$ with the map $\Phi^{r(\delta)}$ with $r(\delta) := a(1-\tau)(p+1-\sigma)$, where σ is any choice of element in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ that raises each root of unity of p-power order to the power $p+1$.

In particular, if we now fix f in $\mathcal{F}^{\mathrm{d}}_{\mathrm{div}}$ and apply the equality (23) with $t = m$, then the above facts imply the existence of a map $\Phi^{r(\delta_{f,m})} \cdot f^{\mathrm{c}}_m \cdot g_{f_m,m}$ in $\mathcal{F}^{\mathrm{c}}$ that agrees with f on $\mu^*_{p^\infty}$, as required to prove claim (v). $\square$

Remark 7.3. By applying an observation of Rubin in [13, §4.8] one can show that the function δ in Proposition 7.2(iii) must satisfy $\delta(m) = 1$ for all even m. Nevertheless, taking f to be a Coleman distribution δ_Π shows that one cannot always take the function δ in Proposition 7.2(iii) to be trivial.

References

[1] J. H. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bull. London Math. Soc. **23** (1991) 321-350.

[2] R. Coleman, Division values in local fields, Invent. Math. **53** (1979) 91-116.

[3] R. Coleman, On an Archimedean characterization of the circular units, J. reine Angew. Math. **356** (1985) 161-173.

[4] R. Gold, J. Kim, Bases for the cyclotomic units, Compositio Math. **71** (1989) 13-27.

[5] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98** (1976) 263-284.

[6] R. Greenberg, On p-adic L-functions and cyclotomic fields, II, Nagoya Math. J. **67** (1977) 139-158.

[7] C. Greither, Class groups of abelian fields and the main conjecture, Ann. Inst. Fourier **42** (1992) 449-499.

[8] C. Greither, On the vanishing of μ-invariants, Appendix to 'The equivariant Tamagawa number conjecture: a survey', M. Flach, Contemp. Math. **358** (2004) 79-126.

[9] D. S. Kubert, S. Lang, Modular Units, Grund. math. Wiss. **244**, Springer-Verlag, New York, 1981.

[10] L. V. Kuz'min, On formulas for the class number of the real abelian fields, Math. USSR - Izv. **60** (1996) 695-761.

[11] K. Rubin, The main conjecture. Appendix to: Cyclotomic Fields I and II, S. Lang, Graduate Texts in Math. **121**, New York: Springer Verlag (1990) 397-419.

[12] K. Rubin, Stark units and Kolyvagin's 'Euler systems', J. Reine Angew. Math. **425** (1992) 141-154.

[13] K. Rubin, Euler systems, Annals of Math. Studies **147**, Princeton Univ. Press, 2000.

[14] A. Saikia, On units generated by Euler systems, Number theory and applications, 157-174, Hindustan Book Agency, New Delhi, 2009.

[15] S. Seo, Circular Distributions and Euler Systems, J. Number Theory **88** (2001) 366-379.

[16] S. Seo, Circular Distributions and Euler Systems, II, Compositio Math **137** (2003) 91-98.

[17] S. Seo, A note on circular distributions, Acta Arith. **114** (2004) 313-322.

[18] S. Seo, Circular distributions of finite order, Math. Res. Lett. **13** (2006) 1-14.

[19] W. Sinnott, On the Stickelberger ideal and circualr units of a cyclotomic field, Ann. Math. **108** (1978) 107-134.

[20] D. R Solomon, Galois Relations for Cyclotomic Numbers and p-Units, J. Number Theory **46** (1994) 158-178.

[21] J. Tate, Les Conjectures de Stark sur les Fonctions L d'Artin en $s = 0$ (notes par D.Bernardi et N. Schappacher), Progress in Math., **47**, Birkhäuser, Boston, 1984.

[22] L. C. Washington, Introduction to Cyclotomic Fields, Grad. Text in Math. **83**, Springer 1982.

King's College London, Department of Mathematics, London WC2R 2LS, U.K.
E-mail address: `david.burns@kcl.ac.uk`

Yonsei University, Department of Mathematics, Seoul, Korea.
E-mail address: `sgseo@yonsei.ac.kr`