ON A CONJECTURE OF COLEMAN
CONCERNING EULER SYSTEMS

DAVID BURNS, ALEXANDRE DAOUD AND SOOGIL SEO

ABSTRACT. We prove a distribution-theoretic conjecture of Robert Coleman, thereby also obtaining an explicit description of the complete set of Euler systems for the multiplicative group over \( \mathbb{Q} \).

1. INTRODUCTION AND STATEMENT OF MAIN RESULT

The theory of distributions plays a prominent role in number theory research and is strongly influenced by the classical theory of circular numbers in abelian fields (see, for example, the discussion of Kubert and Lang in the Introduction to [1]). In this article, we shall prove a distribution-theoretic conjecture of Robert Coleman that has a natural interpretation in terms of the existence of Euler systems for the multiplicative group \( G_{\mathbb{Q}} \).

To be more precise, we write \( \mathbb{Q}^{c} \) for the algebraic closure of \( \mathbb{Q} \) in \( \mathbb{C} \) and \( \mu^{*} \) for the set of non-trivial roots of unity in \( \mathbb{Q}^{c} \). We then recall that a 'circular distribution' is a \( \text{Gal}(\mathbb{Q}^{c}/\mathbb{Q}) \)-equivariant function \( f : \mu^{*} \to \mathbb{Q}^{c} \times \) with the property that

\[
\prod_{\zeta^a = \varepsilon} f(\zeta) = f(\varepsilon)
\]

for all natural numbers \( a \) and all elements \( \varepsilon \) of \( \mu^{*} \).

In the late 1980’s, Coleman formulated a remarkably explicit conjectural description of the complete set of circular distributions. This conjectural description (which we henceforth refer to as ‘Coleman’s Conjecture’) was directly motivated by an archimedean characterization of circular units obtained in [3] and was 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 earlier been proved by Coleman in [3].

To verify Coleman’s Conjecture, we find it convenient to reinterpret the conjecture in terms of a suitable notion of Euler systems. For this purpose we write \( \Omega \) for the set of finite abelian extensions of \( \mathbb{Q} \) in \( \mathbb{Q}^{c} \). For \( E \) and \( E' \) in \( \Omega \) with \( E \subseteq E' \) we write \( N_{E'/E} \) for the field-theoretic norm map \( (E')^{\times} \to E^{\times} \). For a Galois extension \( E \) of \( \mathbb{Q} \) in \( \mathbb{Q}^{c} \) we set \( G_{E} := \text{Gal}(E/\mathbb{Q}) \). For a rational prime \( \ell \) we write \( \sigma_{\ell} \) for the inverse Frobenius automorphism of \( \ell \) on the maximal subextension of \( \mathbb{Q}^{c} \) in which \( \ell \) is unramified. Using this notation, we can now define the Euler systems that are relevant to our purposes.

\[\text{Mathematics Subject Classification. Primary: 11R42; Secondary: 11R27.}\]
Definition 1.1. An Euler system for $G_m$ over $\mathbb{Q}$ is a collection

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

with the property that for every $E$ and $E'$ in $\Omega$ with $E \subset E'$ one has

$$N_{E'/E}(u_{E'}) = (u_E)^{\prod (1 - \sigma_\ell)}$$

in $E^\times$, where in the product $\ell$ runs over the finite set of prime numbers that ramify in $E'$ but not in $E$. We write $ES(G_m)$ for the collection of all such systems.

Remark 1.2. The set $ES(G_m)$ is an abelian group under multiplication of systems (so that the component of $u_1u_2$ at $E$ is equal to the product $u_{1,E}u_{2,E}$), with identity element equal to the system $u_{\text{triv}}$ that has $u_{\text{triv},E} = 1$ for every $E$ in $\Omega$. This group is also endowed with a natural action of the commutative, non-noetherian, ring

$$R := \lim_{\leftarrow E \in \Omega} \mathbb{Z}[G_E],$$

where the transition morphisms in the inverse limit are induced by the natural restriction maps $\mathbb{Z}[G_{E'}] \to \mathbb{Z}[G_E]$ for $E \subset E'$. For $u = (u_E)_E$ in $ES(G_m)$ and $r = (r_E)_E$ in $R$ we write $u^r$ for the system in $ES(G_m)$ that has value $u^r_{E,E}$ at each $E$ in $\Omega$. In a similar way, the set of circular distributions also has a natural multiplicative structure as $R$-module.

Remark 1.3. We caution the reader that, whilst we usually use exponential notation to indicate the action of a commutative ring $\Lambda$ on a multiplicative group $U$, as in (2) and Remark 1.2, we shall also often, for typographic simplicity, use additive notation and hence write either $\lambda(u)$ or $\lambda \cdot u$ in place of $u^\lambda$ for $\lambda \in \Lambda$ and $u \in U$.

To describe some explicit Euler systems (in the above sense), we set

$$\zeta_n := e^{2\pi i/n}$$

and

$$\mathbb{Q}(n) := \mathbb{Q}(\zeta_n) \subset \mathbb{Q}^c$$

for each natural number $n$. We also write $m(E)$ for the finite part of the conductor of each field $E$ in $\Omega$ (so that $E \subseteq \mathbb{Q}(m(E))$).

Example 1.4. For $E$ in $\Omega$ set

$$c_E := N_{\mathbb{Q}(m(E))/E}(1 - \zeta_{m(E)}) \in E^\times.$$ 

Then by substituting $X = \zeta_{mn}$ in the polynomial identities $1 - X^n = \prod_{a=0}^{a=n-1} (1 - \zeta_{ma}^n X)$ for each pair of natural numbers $m$ and $n$ one checks that the ‘cyclotomic Euler system’

$$c := (c_E)_{E \in \Omega}$$

satisfies the distribution relations (2) and so belongs to $ES(G_m)$. This system is known to be directly related to the values of derivatives of Dirichlet $L$-series (cf. [16, Chap. 3, §5]).

Example 1.5. Let $P$ denote the collection of non-empty subsets of the set of all odd prime numbers. For $\Pi$ in $P$ and $E$ in $\Omega$ set

$$u_{\Pi,E} := N_{\mathbb{Q}(m(E))/E}(-1)^{\Pi_{\Pi',E}} \in \{ \pm 1 \},$$
with \( n_{\Pi,E} \) defined to be 1 if \( m(E) \) is divisible only by primes in \( \Pi \) and to be 0 otherwise. Then an explicit check shows that, for each such set \( \Pi \), the ‘Coleman distribution’

\[ u_{\Pi} := (u_{\Pi,E})_{E \in \Omega} \]

satisfies the distribution relations \( \mathcal{E} \) and hence defines an element of \( \text{ES}(\mathbb{G}_m) \) of order two. In the sequel we consider the \( R \)-submodule

\[ T := R \cdot \{ u_{\Pi} : \Pi \in \mathcal{P} \} \]

of \( \text{ES}(\mathbb{G}_m) \) that comprises all finite products of systems \( u_{\Pi} \) for \( \Pi \) in \( \mathcal{P} \).

Having recalled these concrete examples, we can now state an explicit description of the full module \( \text{ES}(\mathbb{G}_m) \).

**Theorem 1.6.** One has \( \text{ES}(\mathbb{G}_m) = T \oplus Rc. \)

This is our main result and, as far as we are aware, is the first explicit description of the complete set of Euler systems in any setting. Further, since Theorem 1.6 implies, modulo minor 2-torsion issues, that every Euler system for \( \mathbb{G}_m \) over \( \mathbb{Q} \) is directly related to the cyclotomic Euler system, and hence to Dirichlet \( L \)-series, it demonstrates the remarkable strength of distribution relations and thereby perhaps helps to explain the great difficulty that there is to construct Euler systems in natural settings.

For each odd prime \( p \), the result of Theorem 1.6 also implies that the \( p \)-adic completion of \( \text{ES}(\mathbb{G}_m) \) is generated over the \( p \)-adic completion \( R_p \) of \( R \) by (the image of) the system \( c \), and hence validates an analogue for \( \mathbb{G}_m \) of the question of whether the \( R_p \)-module of \( p \)-adic Euler systems for \( \mathbb{Z}_p(1) \) is cyclic, as asked by Mazur and Rubin at the end of \([8, \S 5.3]\).

Turning to Coleman’s Conjecture, we note that for any circular distribution \( f \) there exists a unique Euler system \( u_f \) in \( \text{ES}(\mathbb{G}_m) \) with the property that \( u_f, \mathbb{Q}(m) = f(\zeta_m) \) for all \( m > 1 \) with \( m \not\equiv 2 \) (mod 4). The assignment \( f \mapsto u_f \) constitutes an isomorphism between the \( R \)-module of circular distributions and \( \text{ES}(\mathbb{G}_m) \) (for details see the discussion in \( [11, \S 2.1.1] \)) and, via this isomorphism, the result of Theorem 1.6 can be seen to validate the precise statement of Coleman’s Conjecture (as recalled explicitly, for example, in \( [1, \text{Conj. 1.1}] \)).

For the same reason, the description in Theorem 1.6 also implies an affirmative answer to the ‘Guess’ formulated by the third author in \( [13, \S 3] \), thereby providing a natural distribution-theoretic analogue of the main result of Coleman in \( [4] \).

In addition, if \( K \) is the maximal real subfield of \( \mathbb{Q}(n) \) for any natural number \( n \), then the discussion of the third author in \( [14, \S 1] \) shows that Theorem 1.6 combines with results of Sinnott \( [15] \) on cyclotomic units to imply that the cardinality of the graded module of ‘truncated Euler systems’ over \( K \) that is defined in \( [17] \) is equal to the class number of \( K \), as is conjectured in loc. cit.

Finally we note that, in a complementary article, it will be shown that Theorem 1.6 gives concrete information about the structure over (the non-noetherian ring) \( R \) of the Selmer group of \( \mathbb{G}_m \) over the abelian closure of \( \mathbb{Q} \). In this regard, we recall that the latter Selmer group is a classical object in number theory that encodes information about the Galois structures of the ideal class group and unit group of every abelian field.
Remark 1.7. Following Coleman, a circular distribution $f$ is said to be ‘strict’ if for all natural numbers $n$ and all primes $\ell$ that do not divide $n$ it satisfies the congruence relation

$$f(\zeta_\ell^n) \equiv f(\zeta_n^n) \pmod{\text{all primes above } \ell}.$$ 

Such congruence relations also arise naturally in the theory of Euler systems (see, for example, the discussion in [9]). The collection of strict circular distributions corresponds (under the isomorphism discussed above) to the $\mathbb{R}$-submodule $\text{ES}(\mathbb{G}_m)^{\text{str}}$ of $\text{ES}(\mathbb{G}_m)$ comprising systems $u = (u_E)_{E \in \Omega}$ with the property that for all fields $E \subset E'$ for which $m(E') = \ell \cdot m(E)$ with $\ell$ a prime that does not divide $m(E)$ one has $u_{E'} \equiv u_E^{\ell^r} \pmod{\text{all primes above } \ell}$. With $u_{\text{odd}}$ denoting the Coleman distribution corresponding (via the discussion in Example 1.5) to the set $\Pi_{\text{odd}}$ of all odd primes, it follows as an easy consequence of Theorem 1.6 that

$$\text{ES}(\mathbb{G}_m)^{\text{str}} = \{u_{\text{triv}}, u_{\text{odd}}\} \oplus \mathbb{R}c.$$ 

Remark 1.8. In [2] Coates introduced an analogue of the notion of circular distributions in the setting of abelian extensions of imaginary quadratic fields and it seems likely the methods used here could be further developed in order to prove an analogue of Theorem 1.6 in that setting.

2. The proof of Theorem 1.6

Our proof of Theorem 1.6 will follow a general approach to Coleman’s Conjecture that was developed by the first and third authors in [1].

In contrast to this earlier approach, however, we focus here on the study of individual Euler systems rather than on families of Euler systems and are thereby able to reduce verification of the conjecture to a natural $p$-adic problem for every prime $p$. This key reduction is explained in §2.3 and relies critically both on aspects of the Galois structure of modules of cyclotomic elements (that follow from the link between cyclotomic elements and Dirichlet $L$-series) and the fact that the Euler systems that are relevant to Coleman’s Conjecture have components in abelian fields of arbitrary conductor.

Having made this reduction, the individual $p$-adic problems are then resolved by combining a delicate analysis of pro-$p$ completions together with results from [1] which themselves rely on detailed properties of Euler systems that are established by Rubin in [10] and by Greither in [5].

In the sequel, we write $A_{\text{tor}}$ for the torsion subgroup of an abelian group $A$.

2.1. Initial observations. At the outset we recall it is proved by the third author in [13, Th. 2.5] that the group $Rc$ is torsion-free and hence that $T \cap Rc = \{0\}$.

To prove Theorem 1.6 it is therefore enough for us to show that each system $v$ in $\text{ES}(\mathbb{G}_m)$ belongs to $T + Rc$. Our proof of this fact (for a system $v$ that is henceforth regarded as fixed) will occupy the remainder of this article.

In this first section we make several useful deductions from results of [1]. To do this we write $\tau$ for the element of $\mathbb{G}_{\mathbb{Q}_c}$ induced by complex conjugation and then define $R$-modules

$$C := Rc^{1 + \tau}, \quad Y := Rv^{1 + \tau} \quad \text{and} \quad X := (C + Y)/C.$$ 

The following result shows that Theorem 1.6 is equivalent to asserting that the module $X$ vanishes.
Lemma 2.1. There exists a canonical exact sequence

\[ 0 \to T + Rc \xrightarrow{\iota} T + Rc + Rv \xrightarrow{\pi} X \to 0 \]

Proof. Since \( y^{1+\tau} = 0 \) for every \( y \in T \) one has \( z^{1+\tau} \in C + Y \) for each \( z \in T + Rc + Rv \) and so one obtains a well-defined surjective homomorphism of \( R \)-modules \( t \) by sending each \( z \) to the class of \( z^{1+\tau} \) in \( X \).

With this definition of \( t \), it is clear \( T + Rc \) is contained in \( \ker(t) \) and hence enough to show that if \( t(z) = 0 \), then \( z \) belongs to \( T + Rc \).

Now if \( t(z) = 0 \), then there exists an element \( r \) of \( R \) such that \( z^{1+\tau} = (c^{1+\tau})^r \). It follows that \( (zc^{-r})^{1+\tau} = 1 \) and hence, by \([1\text{ Th. 4.1(i)}] \), that \( zc^{-r} \) belongs to \( \text{ES}(\mathbb{G}_m)_\text{tor} + Rc^{1-\tau} \).

Since this implies \( z \) belongs to \( \text{ES}(\mathbb{G}_m)_\text{tor} + Rc \), it is therefore enough to note that in \([12\text{ Th. B}] \) the third author has proved \( \text{ES}(\mathbb{G}_m)_\text{tor} \) is equal to \( T \). \( \square \)

The following property of \( X \) will also play a key role in the sequel.

Lemma 2.2. \( X \) is torsion-free.

Proof. The module \( X \) identifies with a subgroup of the quotient \( Q \) of \( \text{ES}(\mathbb{G}_m)^{1+\tau} \) by \( R \cdot c^{1+\tau} \).

In addition, one knows that \( Q \) is torsion-free since, for every prime \( p \), it is isomorphic to a subgroup of a uniquely \( p \)-divisible group, as a direct consequence of claims (i) and (ii) of \([1\text{ Th. 5.1}] \). \( \square \)

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

We write \( \# X \) for the cardinality of a finite set \( X \). If \( \Gamma \) is a finite group, then we write \( e_\Gamma \) for the idempotent \( e_\Gamma := \#\Gamma^{-1} \cdot \sum_{\gamma \in \Gamma} \gamma \) of \( \mathbb{Q}[\Gamma] \), and for each homomorphism \( \chi : \Gamma \to \mathbb{Q}^{\times} \) we write \( e_\chi \) for the primitive idempotent \( (\#\Gamma)^{-1} \sum_{\gamma \in \Gamma} \chi(\gamma^{-1}) \gamma \) of \( \mathbb{Q}[\Gamma] \).

For each field \( L \) in \( \Omega \) we write \( L^+ \) for its maximal real subfield and set \( \mathcal{G}_L^+ := \mathcal{G}_L^+ \). We then define an ideal of \( \mathbb{Z}[\mathcal{G}_L^+] \) by setting

\[ I_L := \{ r \in \mathbb{Z}[\mathcal{G}_L^+] : r(c^{1+\tau}) = 0 \}. \]

In the following result we shall describe explicitly this annihilator ideal in terms of the idempotent of \( \mathbb{Q}[\mathcal{G}_L^+] \) that is obtained by setting

\[ e_L := \begin{cases} 
1, & \text{if } m(L) \text{ is a prime power}, \\
\prod_{\ell \mid m(L)} (1 - e_{\mathcal{D}_L \ell}), & \text{otherwise},
\end{cases} \]

where in the product \( \ell \) runs over all prime divisors of \( m(L) \) and \( D_{L,\ell} \) denotes the decomposition subgroup of \( \ell \) in \( \mathcal{G}_L^+ \).

Proposition 2.3. For every field \( L \) in \( \Omega \) the following claims are valid.

(i) \( I_L \) is equal to the set \( \{ x \in \mathbb{Z}[\mathcal{G}_L^+] : e_L \cdot x = 0 \} \).

(ii) If \( \psi : \mathcal{G}_L^+ \to \mathbb{Q}^{\times} \) is any homomorphism such that \( e_\psi e_L = 0 \), then \( m(L) \) is not a prime power and \( \psi \) is trivial on the decomposition group in \( \mathcal{G}_L^+ \) of at least one prime divisor of \( m(L) \).

(iii) If \( u \) belongs to \( \text{ES}(\mathbb{G}_m)^{1+\tau} \), then the image of \( u_L \) in \( \mathbb{Q} \otimes \mathbb{Z}^{L^\times} \) belongs to the \( \mathbb{Q}[\mathcal{G}_L^+] \)-module generated by \( c^{1+\tau} \).
Proof. Claim (i) is proved in [11 Lem. 2.4] and relies on the fundamental link between cyclotomic elements and first derivatives of Dirichlet $L$-series (as discussed, for example, in [16 Chap. 3, §5]).

Claim (ii) follows directly from the explicit description [3] of $e_L$ and the fact that for each subgroup $H$ of $G^+_L$ one has $e_\psi(1 - e_H) = 0$ if $\psi$ is trivial on $H$ and $e_\psi(1 - e_H) = e_\psi$ otherwise.

To prove claim (iii) we use the fact that the natural map $\psi : L^\times \to Q_\ell \otimes \mathbb{Z} L^\times$ is injective on the torsion-free subgroup $(L^\times)^{1+\tau}$ of $L^\times$. We write $u = w^{1+\tau}$ with $w \in ES(\mathbb{G}_m)$ and claim first that the image of $u_L = w_L^{1+\tau}$ under $\pi$ is stable under multiplication by $e_L$. In view of claim (ii), to show this it is enough to prove for every homomorphism $\psi : G^+_L \to Q_\ell^{c, \times}$ that if $e_\psi(\pi(u_L)) \neq 0$, then $\psi$ cannot be trivial on the decomposition group of any prime that ramifies in $L$ (and so $e_\psi e_L = e_\psi$).

To see this, we write $\pi$ for the restriction map $G_L \to G^+_L$ and then note that, for each homomorphism $\psi : G^+_L \to Q_\ell^{c, \times}$, one has

$$e_\psi(\pi(u_L)) = e_{\psi \circ \pi}(\pi(u_L))^{1+\tau} = 2 \cdot e_{\psi \circ \pi}(\pi(u_L)) = 2 \cdot \left( \prod_{\ell \in P_\psi} (1 - \psi(\sigma_\ell, L_\psi)) \right) e_{\psi \circ \pi}(\pi(u_L)) = \left( \prod_{\ell \in P_\psi} (1 - \psi(\sigma_\ell, L_\psi)) \right) e_{\psi}(\pi(u_L)).$$

Here $L_\psi$ denotes the subfield of $L$ fixed by $\ker(\psi \circ \pi)$ (or equivalently, the subfield of $L^+$ fixed by $\ker(\psi)$), $P_\psi$ is the set of primes that ramify in $L$ but not in $L_\psi$ and for each $\ell$ in $P_\psi$ we write $\sigma_\ell, L_\psi$ for the image of $\sigma_\ell$ in $G^+_L$. In addition, the first of the equalities is clear, the second and fourth are true since the image of $\pi$ in $G^+_L$ is contained in $\ker(\psi \circ \pi)$, and the third equality is true since the system $w$ validates the distribution relation [2].

From the above equalities it is clear that, if $e_\psi(\pi(u_L)) \neq 0$, then $\ker(\psi)$ cannot contain $\sigma_\ell, L_\psi$ for any $\ell$ in $P_\psi$. On the other hand, any prime $\ell$ that ramifies in $L$ but does not belong to $P_\psi$ is ramified in $L_\psi$ and so its inertia group in $G^+_L$ is not contained in $\ker(\psi)$. Hence, if $e_\psi(\pi(u_L)) \neq 0$, then $\psi$ cannot be trivial on the decomposition group in $G^+_L$ of any prime that ramifies in $L$, as required.

To proceed we write $S(L)$ for the set of archimedean places of $L$, respectively the set of places of $L$ that are either archimedean or $p$-adic, if $m(L)$ is divisible by two distinct primes, respectively if $m(L)$ is a power of a prime $p$. We then write $U'_L$ for the (finitely generated) subgroup of $L^\times$ comprising elements that are units at all places of $L$ outside $S(L)$ and $X'_L$ for the subgroup of the free abelian group on $S(L)$ comprising elements whose coefficients sum to zero.

Then we recall that the distribution relation [2] implies $w_L$ belongs to $U'_L$ (for a proof of this fact see, for example, [11 Lem. 2.2]) and hence, in view of the above argument, that $\pi(u_L)$ belongs to $e_L(\mathbb{Q} \otimes \mathbb{Z} (U'_L)^{1+\tau})$. 


To prove claim (iii) it is thus enough to show that the \( \mathbb{Q}[G_L^+] \)-module \( e_L(\mathbb{Q} \otimes \mathbb{Z} (U'_L)^{1+\tau}) \) is generated by \( c_L^{1+\tau} \). But this is true since if \( \psi \) is any homomorphism \( \hat{G}_L^+ \rightarrow \mathbb{Q}^{c,x} \) for which \( e_L \psi e_L \neq 0 \), then claim (i) combines with the observation that \( c_L \) belongs to \( U'_L \) to imply that \( e_L(\psi(c_L^{1+\tau})) \) is a non-zero element of \( e_L(\mathbb{Q}^c \otimes \mathbb{Z} (U'_L)^{1+\tau}) \), whilst one also knows that

\[
\dim_{\mathbb{Q}^c}(e_L(\mathbb{Q}^c \otimes \mathbb{Z} (U'_L)^{1+\tau})) = \dim_{\mathbb{Q}^c}(e_L(\mathbb{Q}^c \otimes \mathbb{Z} X'_L)) = 1,
\]

where the first equality is true since the Dirichlet Regulator map induces an isomorphism of \( \mathbb{C}[G_L] \)-modules \( \mathbb{C} \otimes \mathbb{Z} U'_L \cong \mathbb{C} \otimes \mathbb{Z} X'_L \) (cf. [16, Chap. I, §4.2]) and the second follows by a straightforward computation from the definition of \( X'_L \).

\[\square\]

2.3. The reduction of Theorem 1.6 to \( p \)-primary considerations. By the discussion in §2.1 the proof of Theorem 1.6 is reduced to showing that the group \( X \) vanishes. In this section we reduce the vanishing of \( X \) to a family of \( p \)-primary problems.

2.3.1. For an abelian group \( A \) we set

\[\hat{A} := \varprojlim_{n \in \mathbb{N}} A/nA \text{ and } \hat{A}^p := \varprojlim_{m \in \mathbb{N}} A/p^m A\]

for each prime \( p \), where all limits are taken with respect to the natural projection maps (and, for typographic simplicity, we sometimes write \( A^{\hat{\land} p} \) in place of \( \hat{A}^p \)). We use similar notation for homomorphisms of abelian groups. We also note that if \( A \) is finitely generated, then \( \hat{A} \) and \( \hat{A}^p \) respectively identify with the tensor products \( A \otimes \mathbb{Z} \hat{\mathbb{Z}} \) and \( A \otimes \mathbb{Z} \mathbb{Z}_p \).

The following result records some elementary properties of the functors \( A \mapsto \hat{A} \) and \( A \mapsto \hat{A}^p \) that will be useful in the sequel.

**Lemma 2.4.** If \( A \) is a torsion-free abelian group, then the following claims are valid.

\[(i) \text{ If } 0 \rightarrow A_1 \xrightarrow{\theta} A_2 \xrightarrow{\phi} A \rightarrow 0 \text{ is an exact sequence of abelian groups, then the induced sequences } 0 \rightarrow \hat{A}_1 \xrightarrow{\hat{\theta}} \hat{A}_2 \xrightarrow{\hat{\phi}} \hat{A} \rightarrow 0, \text{ and } 0 \rightarrow \hat{A}_1^p \xrightarrow{\hat{\theta}^p} \hat{A}_2^p \xrightarrow{\hat{\phi}^p} \hat{A}^p \rightarrow 0 \text{ for each prime } p, \text{ are also exact.}\]

\[(ii) \text{ The groups } \hat{A}, \text{ and } \hat{A}^p \text{ for each prime } p, \text{ are torsion-free.}\]

\[(iii) \text{ For each prime } p, \text{ the natural map } \hat{A}^p \rightarrow (\hat{A}^p)^{\hat{\land} p} \text{ is bijective.}\]

**Proof.** For both claims (i) and (ii), it is enough to consider the functor \( A \mapsto \hat{A} \).

To prove claim (i) in this case we note first that, since \( A \) is torsion-free, for each natural number \( n \) the Snake Lemma applies to the following exact commutative diagram

\[
\begin{array}{ccc}
0 & \rightarrow & A_1 \xrightarrow{\theta} A_2 \xrightarrow{\phi} A \xrightarrow{n} 0 \\
\downarrow n & & \downarrow n & \downarrow n \\
0 & \rightarrow & A_1 \xrightarrow{\theta} A_2 \xrightarrow{\phi} A \xrightarrow{0} 0
\end{array}
\]

to give an exact sequence \( 0 \rightarrow A_1/nA_1 \xrightarrow{\theta/n} A_2/nA_2 \xrightarrow{\phi/n} A/nA \rightarrow 0 \). It is then enough to note that the latter sequences are compatible (with respect to the natural projection maps) as \( n \) varies and that, by the Mittag-Leffler criterion, exactness of the sequences is preserved
when one passes to the inverse limit over $n$ since, for each multiple $m$ of $n$ the projection map $A_1/mA_1 \to A_1/nA_1$ is surjective.

To prove claim (ii) we must show that if $x = (x_n)_n$ is an element of $\hat{A}$ with the property that $px = 0$ for some prime $p$, then $x = 0$. But, since $A$ is torsion-free, for each $n$ the element $x_{np}$ is the image in $A/(npA)$ of an element $\hat{x}_{np}$ of $nA$. Since $x_n$ is equal to the image of $\hat{x}_{np}$ in $A/(nA)$ one therefore has $x_n = 0$, as required.

Finally, we note that claim (iii) is both straightforward to prove directly and also follows immediately from the general result [7, Th. 15] of Matlis (since $\hat{A}^p$ is equal to the completion of the $\mathbb{Z}$-module $A$ at the ideal generated by $p$).

\[ \Box \]

2.3.2. In the sequel we set $R^+_L := \mathbb{Z}[G^+_L]$ for each $L$ in $\Omega$ and consider the inverse limits

\[ R^+ := \lim_{\leftarrow L \in \Omega} R^+_L \quad \text{and} \quad \hat{R}^+ := \lim_{\leftarrow L \in \Omega} \hat{R}^+_L \]

where, in both cases, the transition morphisms are the natural projection maps.

The following result is the main observation that we make in this section and will play a key role in the proof of Theorem 1.6.

**Proposition 2.5.** *The diagonal map $X \rightarrow \prod_p \hat{X}^p$, where $p$ runs over all primes, is injective.*

**Proof.** The Chinese Remainder Theorem implies that the natural map $\hat{X} \rightarrow \prod_p \hat{X}^p$ is injective and so it is enough to prove that this is also true of the natural map $\iota : X \rightarrow \hat{X}$.

Recalling that $C$ and $Y$ respectively denote the modules $Rc^{1+\tau} = R^+c^{1+\tau}$ and $Rv^{1+\tau} = R^+v^{1+\tau}$, we consider the following exact commutative diagram

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & C & \xrightarrow{c} & C + Y & \xrightarrow{\pi} & X & \longrightarrow & 0 \\
& & \downarrow{\iota_2} & & \downarrow{\iota_1} & & \downarrow{\iota} & & \\
0 & \longrightarrow & \hat{C} & \xrightarrow{c} & (C + Y)^\wedge & \xrightarrow{\hat{\pi}} & \hat{X} & \longrightarrow & 0.
\end{array}
\]

The top row of this diagram is the tautological short exact sequence, all vertical maps are the natural maps and the lower row is the short exact sequence that is induced by applying Lemma 2.4(i) to the upper row and recalling that $X$ is torsion-free (by Lemma 2.2).

The map $\iota_1$, and hence also $\iota_2$, is injective. This follows easily from the equality $\ker(\iota_1) = \bigcap_{n \in \mathbb{N}} n(C + Y)$ and the fact that for every $x$ in $C + Y$ and every $L$ in $\Omega$ the component $x_L$ of $x$ at $L$ belongs to the finitely generated group $U'_L$ defined in the proof of Proposition 2.3(iii).

We use $\iota_2$ and $\iota_1$ to regard $C$ and $C + Y$ as subgroups of $\hat{C}$ and $(C + Y)^\wedge$ respectively, and then apply the Snake Lemma to the above diagram to deduce that the kernel of $\iota$ is isomorphic to the quotient of $\hat{C} \cap (C + Y)$ by $C$, where the intersection takes place in $(C + Y)^\wedge$.

To prove the claimed result we are therefore reduced to proving an equality

\[ \hat{C} \cap (C + Y) = C. \]


To check this we note that the map $R^+ \to C$ sending each element $r$ to $(e_1^+)^r$ is bijective (as a consequence of [1, Th. 1.2]) and hence extends to give an isomorphism $\hat{R}^+ \cong \hat{C}$ of $\hat{R}^+$-modules.

It follows that every element of $\hat{C}$ is of the form $(e_1^+)^{\lambda}$ with $\lambda = (\lambda_L)_L$ in $\hat{R}^+$ and if such an element belongs to $C + Y$, and hence to ES($\mathbb{G}_m$)$^{1+}$, then Proposition 2.3(iii) implies that for each $L$ there exists a natural number $n_L$ such that $((e_1^+)^{\lambda_L})^{n_L}$ belongs to the $R^+_L$-module $C_L$ that is generated by $e_1^{1+}$. Thus, since $(e_1^+)^{\lambda_L}$ belongs to $\hat{C}_L$ and the quotient $\hat{C}_L/C_L \cong C_L \otimes \mathbb{Z} (\hat{\mathbb{Z}}/\mathbb{Z})$ is torsion-free, it follows that $(e_1^+)^{\lambda_L}$ belongs to $C_L$. Since the annihilator of $e_1^{1+}$ in $R^+_L = \hat{\mathbb{Z}} \otimes \mathbb{Z} R_L^+$ is equal to $\hat{I}_L$ (as $\hat{\mathbb{Z}}$ is a flat $\mathbb{Z}$-module), there must therefore exist an element $r_L$ of $R^+_L$ such that $\lambda_L - r_L \in \hat{I}_L$.

It therefore remains to show that

$$\hat{R}^+ \cap \prod_{L \in \Omega} (R_L^+ + I_L) = R^+. \tag{5}$$

To prove this equality we regard both $\hat{\mathbb{Z}} = \prod_{\ell} \mathbb{Z}_\ell$ and $\mathbb{Q}$ as subgroups of $\prod_{\ell} \mathbb{Q}_\ell$ (where the products are over all primes $\ell$) in the natural way and note that, with these identifications, one has $\hat{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. To justify (5) it is therefore enough to show that if $\lambda = (\lambda_L)_L$ is any element of $\hat{R}^+$ with the property that $\lambda_L \in R_L^+ + \hat{I}_L$ for every $L \in \Omega$, then in fact one has $\lambda_L \in \mathbb{Q}[G_L^+]$ for every $L$. To prove this we shall argue by induction on the number of prime factors of the finite part $m(L)$ of the conductor of $L$.

If, firstly, $m(L)$ is a prime power, then the idempotent $e_L$ is equal to 1 so Proposition 2.3(i) implies $I_L$ vanishes and hence the given assumptions imply that $\lambda_L$ belongs to $R_L^+$, and hence also to $\mathbb{Q}[G_L^+]$ as required.

Now assume to be given a natural number $n$ and suppose that for every field $L$ in $\Omega$ such that $m(L)$ is divisible by at most $n$ primes, one has $\lambda_L \in \mathbb{Q}[G_L^+]$. Fix a field $F$ in $\Omega$ such that $m(F)$ is divisible by $n + 1$ primes. We write $E$ for the set of homomorphisms $G_F^+ \to \mathbb{Q}^\times$ and for each $\psi$ in $E$ we write $F_\psi$ for the fixed field of $F^+$ under $\ker(\psi)$. We note that, for each subfield $E$ of $F^+$ the subset $E(E)$ of $E$ comprising all $\psi$ for which $F_\psi = E$ is a (possibly empty) conjugacy class for the natural action of $G_E$ on $E$ and hence that the associated idempotent $e_E := \sum_{\psi \in E(E)} e_\psi$ belongs to $\mathbb{Q}[G_E^+]$.

To investigate $\lambda_E$ we use the decomposition

$$\lambda_E = 1 \cdot \lambda_E = \left( \sum_{\psi \in E} e_\psi \right) \cdot \lambda_E = \sum_{\psi \in E} e_\psi \lambda_E$$

$$= \sum_{\psi \in E} e_\psi \lambda_{F_\psi} = \sum_{E} \left( \sum_{\psi \in E(E)} e_\psi \lambda_E \right) = \sum_{E} e_E \lambda_E,$$

where the fourth equality is valid since $\lambda$ belongs to $\hat{R}^+$, and in the sum $E$ runs over all subfields of $F^+$.

Fix a subfield $E$ of $F^+$. If $m(E)$ is divisible by fewer primes than $m(F)$ then, by hypothesis, one has that $\lambda_E \in \mathbb{Q}[G_E]$. On the other hand, if $m(E)$ is divisible by the same number
of primes as $m(F)$, and $r_F \in R_F^+$ and $i_F \in \hat{I}_F$ are such that $\lambda_F = r_F + i_F$, then one has

$$\varepsilon_E^* \lambda_E = \sum_{\psi \in \Xi(E)} e_\psi \lambda_E = \sum_{\psi \in \Xi(E)} e_\psi \lambda_F = \sum_{\psi \in \Xi(E)} e_\psi (r_F + i_F) = \sum_{\psi \in \Xi(E)} e_\psi r_F = \varepsilon_F^* r_F,$$

where the fourth equality is valid since, under the present hypothesis, each $\psi$ in $\Xi(E)$ is not trivial on the decomposition group of any prime divisor of $m(F)$ so that one has $e_\psi = e_\psi \epsilon_{F \mid E}$ (by Proposition 2.3(ii)) and hence also $e_\psi (i_F) = 0$ as a consequence of Proposition 2.3(i).

These observations imply that the element $\varepsilon_E^* \lambda_E$ belongs to $\mathbb{Q}[G_F^+]$ for every subfield $E$ of $F^+$ and hence, via the decomposition (6), that $\lambda_F$ belongs to $\mathbb{Q}[G_F^+]$, as required to complete the proof of the Proposition.

\[\square\]

2.4. Euler systems of prime level. The results of Lemma 2.4 and Proposition 2.5 combine to imply that Theorem 1.6 is true provided the group $\hat{X}^p$ vanishes for every prime $p$.

In this section we reinterpret the vanishing of $\hat{X}^p$ in terms of an explicit restriction on the components of the system $v^{1+\tau}$ at fields containing $\mathbb{Q}(p)$.

To do this we fix a prime $p$ and write $\Omega(p)$ for the subset of $\Omega$ comprising fields that contain $\mathbb{Q}(p)$. We then define the collection $ES(p)(\mathbb{G}_m)$ of ‘Euler systems of level $p$’ to be the set of elements $x = (x_L)_{L \in \Omega(p)}$ that are defined just as in Definition 1.1 except that all occurrences of $\Omega$ are replaced by $\Omega(p)$, and we write

$$\varrho : ES(\mathbb{G}_m) \to ES(p)(\mathbb{G}_m)$$

for the ‘restriction’ map that sends each $(x_L)_{L \in \Omega}$ in $ES(\mathbb{G}_m)$ to $(x_L)_{L \in \Omega(p)}$.

We also set

$$\mathcal{E} = \mathcal{E}(p) := ES(p)(\mathbb{G}_m)^{1+\tau},$$

write $\lambda : \mathcal{E} \to \mathcal{E}^{\wedge, p}$ for the natural map and then for each system $x$ in $ES(\mathbb{G}_m)$ we define

$$x(p) := \lambda(\varrho(x^{1+\tau})) \in \mathcal{E}^{\wedge, p}.$$

Finally we set

$$R_p^+ := \lim_{L \in \Omega(p)} Z_p[G_L^+],$$

where the transition morphisms $L \subset L'$ in the limit are the natural projection maps.

**Proposition 2.6.** Write $\kappa$ for the inclusion of $Rc_{(p)} \cap Rv_{(p)}$ into $Rv_{(p)}$. Then the following claims are valid.

(i) The $R$-module $X$ is isomorphic to $cok(\kappa)$.

(ii) The natural map $cok(\hat{R}^p) \to cok(\kappa)^{\wedge, p}$ is bijective.

(iii) For every element $x$ of $Rc + Rv$, the natural map $R_p^+ x_{(p)} \to (Rx_{(p)})^{\wedge, p}$ is bijective.

(iv) Define subgroups of $\mathcal{E}^{\wedge, p}$ by setting $Z := Rc_{(p)} + Rv_{(p)}$ and $Z_p := R_p^+ c_{(p)} + R_p^+ v_{(p)}$. Then, with respect to the identifications in claim (iii), the image of $\hat{R}^p$ is equal to the set of elements $y$ of $R_p^+ v_{(p)}$ which have the same image as an element of $R_p^+ c_{(p)}$ under the natural map $Z_p \to \hat{Z}^p$.

(v) The group $\hat{X}^p$ vanishes if there exists an element of $R_p^+ c_{(p)}$ that has the same image as $v_{(p)}$ under the map $Z_p \to \hat{Z}^p$ that occurs in claim (iv).
Proof. To prove claim (i) we note that the association \( x \mapsto \lambda(\rho(x)) \) induces a well-defined homomorphism of \( R \)-modules \( t \) from \( X = (Rc^{1+\tau} + Rv^{1+\tau})/Rc^{1+\tau} \) to the quotient \( Q \) of \( Rc(p) + Rv(p) \) by \( Rv(p) \). Since \( Q \) is naturally isomorphic to \( \text{cok}(\kappa) \), it is thus enough to show that this map \( t \) is bijective. Since \( t \) is clearly surjective it is therefore enough to show that if \( z \) is any element of \( Rc^{1+\tau} + Rv^{1+\tau} \) such that \( \lambda(\rho(z)) \) belongs to \( Rc(p) \), then \( z \) belongs to \( Rc^{1+\tau} \).

To prove this we note first that \( \lambda \) is injective. This is true since for every \( x \) in \( \mathcal{E} \) the component \( x_L \) at each field \( L \) in \( \Omega(p) \) belongs to the finitely generated torsion-free abelian group \((U_L')^{1+\tau} \). (We note in passing that this observation also implies that the group \( \mathcal{E} \), and hence, by Lemma 2.4(ii), also \( \mathcal{E}^{\wedge_p} \), is torsion-free).

The injectivity of \( \lambda \) implies that if \( \lambda(\rho(z)) = c_{(p)} = \lambda(\rho(c^{1+\tau})) \) for some \( r \) in \( R \), then the system \( zc^{-(1+\tau)r} \) belongs to both \( ES(G_m)^{1+\tau} \) and \( \ker(\rho) \). Thus, after converting between the notions of Euler system and circular distribution (as per the discussion in \( [\text{11}] \)), we can apply the result of \( [\text{11}] \) Lem. 2.1] (in which we take \( \Sigma \) to be the set of multiples of \( p \), and we note that the notion of ‘circular distribution of level \( p \)’ in loc. cit. corresponds to our notion of Euler system of level \( p \)) in order to deduce that \( zc^{-(1+\tau)r} = 1 \). This equality in turn implies that \( z = c^{(1+\tau)r} \) belongs to \( Rc^{1+\tau} \), as required to prove claim (i).

To prove claim (ii) we note that the isomorphism in claim (i) combines with Lemma 2.2 to imply \( \text{cok}(\kappa) \) is torsion-free. Given this, the tautological exact sequence

\[
0 \to Rc(p) \cap Rv(p) \xrightarrow{\kappa} Rv(p) \to \text{cok}(\kappa) \to 0
\]

combines with Lemma 2.4(i) to imply that the induced sequence

\[
0 \to (Rc(p) \cap Rv(p))^{\wedge_p} \xrightarrow{\kappa^p} (Rv(p))^{\wedge_p} \to \text{cok}(\kappa)^{\wedge_p} \to 0
\]

is exact, and this immediately implies the isomorphism in claim (ii).

To prove claim (iii) we fix \( x \in Rc + Rv \) and for \( L \) in \( \Omega(p) \) write \( J_L \) for the annihilator of \( x^+_L \) in \( \mathbb{Z}[G_L^+] \). Then an element \( r = (r_L)_{L \in \Omega(p)} \) of \( R^+ = \varprojlim_{L \in \Omega(p)} \mathbb{Z}[G_L^+] \) annihilates \( x_L \) if and only if \( r_L \in J_L \) for every \( L \) in \( \Omega(p) \) and so the annihilator of \( x(p) \) in \( R^+ \) is equal to the ideal \( J := \varprojlim_{L \in \Omega(p)} J_L \). Since the \( R \)-module generated by \( x(p) \) is torsion-free, Lemma 2.4(i) gives rise to an exact sequence of \( R_p^+ \)-modules

\[
0 \to \hat{J}^p \xrightarrow{\kappa} R_p^+ \xrightarrow{(Rx(p))^{\wedge_p}} 0
\]

in which the third arrow sends 1 to the image of \( x(p) \) in \( (Rx(p))^{\wedge_p} \).

Next we note that, since \( \mathbb{Z}_p \) is flat over \( \mathbb{Z} \), for each \( L \) in \( \Omega(p) \) the annihilator in \( \mathbb{Z}_p[G_L^+] \) of the \( L \)-component of \( x(p) \) is equal to \( J_{L,p} := \mathbb{Z}_p \otimes \mathbb{Z} J_L \). This implies that there is an exact sequence of \( R_p^+ \)-modules

\[
0 \to J_p \xrightarrow{\kappa} R_p^+ \xrightarrow{R_p^+x(p)} 0
\]

where we set \( J_p := \varprojlim_{L \in \Omega(p)} J_{L,p} \) and the third arrow sends 1 to \( x(p) \).

Now the groups \( (Rx(p))^{\wedge_p} \) and \( R_p^+x(p) \) are torsion-free and for each \( n \) the natural map

\[
((Rx(p))^{\wedge_p})/p^n \to Rx(p)/p^n = (R_p^+x(p))/p^n
\]
is bijective. Hence, if we take cokernels under multiplication by $p^n$ of the sequences (7) and (8) we obtain an equality
\[ \hat{J}_p/p^n = J_p/p^n. \]
In addition, from the exactness of each sequence
\[ 0 \to J_{L,p} \xrightarrow{p^n} J_{L,p} \to J_{L,p}/p^n \to 0, \]
and the compactness of each module $J_{L,p}$, one finds that
\[ J_p/p^n = \lim_{L \in \Omega(p)} (J_{L,p}/p^n). \]
Upon combining these observations, one deduces that
\[ \hat{J}_p = \lim_{n} (\hat{J}_p/p^n) = \lim_{n} (\lim_{L \in \Omega(p)} (J_{L,p}/p^n)) = \lim_{L \in \Omega(p)} \lim_{n} (J_{L,p}/p^n) = \lim_{L \in \Omega(p)} J_{L,p} = J_p, \]
where the first equality is valid by Lemma 2.4(iii) and the fourth since $J_{L,p} = (J_L)^{\wedge,p}$ as $J_L$ is finitely generated. Then, since $\hat{J}_p = J_p$, the assertion of claim (iii) follows directly upon comparing the exact sequences (7) and (8).

To prove claim (iv) we consider the submodule $W := R\kappa(p) \cap R\nu(p)$ of $E$ and use the exact sequence of $R$-modules
\[ 0 \to W \xrightarrow{x \mapsto (x,x)} R\kappa(p) \oplus R\nu(p) \xrightarrow{\theta} Z \to 0 \]
in which $\theta$ sends each element $(x, y)$ to $x - y$. Now, since $E$, and hence also $Z$, is torsion-free this sequence combines with Lemma 2.4(i) and the isomorphisms in claim (iii) to imply exactness of the row in the following commutative diagram
\[ \begin{array}{cccccccc}
0 & \to & \hat{W}^p & \xrightarrow{x \mapsto (x,x)} & R_p^+ c_{(p)} \oplus R_p^+ v_{(p)} & \xrightarrow{\hat{\theta}^p} & \hat{Z}^p & \to 0 \\
& & \downarrow{\hat{\kappa}^p} & & \downarrow{(x,y) \mapsto y} & & \downarrow{R_p^+ v_{(p)}}
\end{array} \]
This exact diagram leads directly to the explicit description of $\text{im}(\hat{\kappa}^p)$ given in claim (iv).

Finally, to verify claim (v), we note that claim (i) implies $\hat{X}_p$ vanishes if $\text{cok}(\kappa)^{\wedge,p}$ vanishes and hence therefore, by claim (ii), if the map $\hat{\kappa}^p$ is surjective. Claim (v) is therefore true since claim (iv) implies that $\hat{\kappa}^p$ is surjective if there exists an element of $R_p^+ c_{(p)}$ that has the same image as $v_{(p)}$ under the natural map $Z_p \to \hat{Z}^p$. □

2.5. Completion of the proof. In view of Lemma 2.1, Proposition 2.5 and Proposition 2.6(v), to prove Theorem 1.6 it is enough to show that, for every prime $p$, the restricted system $v_{(p)}$ belongs to $R_p^+ c_{(p)}$. We shall now explain how the latter claim follows as a consequence of results in [1].

As a first step we note that, after converting between the notions of circular distribution and Euler system (just as in the proof of Proposition 2.6(i)), the result of [1] Th. 3.1] implies that for each field $L$ in $\Omega(p)$ there exists an element $r_L$ of $Z_p[GL]$ such that $v_L = r_L(c_L)$ in $Z_p \otimes_Z U'_L$ and hence also \[ v_L^{1+\tau} = r_L^{c_L^{1+\tau}} \]
in \( Z_p \otimes_{\mathbb{Z}} (U'_L)^{1+\tau} \), where \( r^+_L \) denotes the projection of \( r_L \) to \( Z_p[G^+_L] \).

Now, since the system \( \tilde{v} := (v^{1+\tau})_{L \in \Omega(p)} \) both belongs to the group \( E = ES(p)(G_m)^{1+\tau} \) discussed in §2.4 and verifies the above displayed equality (for a suitable choice of element \( r^+_L \) of \( Z_p[G^+_L] \)) for every \( L \) in \( \Omega(p) \), it defines an element of the group \( \mathcal{V}^d \) discussed in [1 §5.3.1]. Hence, as the result of [1 Prop. 5.3(i)] (in which the algebra \( R^+_p \) is denoted by \( \Lambda(p) \)) implies that \( \mathcal{V}^d \) is a free module over \( R^+_p \), with basis given by the element \( \tilde{c} := (c^{1+\tau})_{L \in \Omega(p)} \) of \( E \), there exists an element \( r_p = (r_{p,L})_{L \in \Omega(p)} \) of \( R^+_p \) with the property that, for every \( L \) in \( \Omega(p) \), one has

\[
(9) \quad v^{1+\tau}_L = r_{p,L}(c^{1+\tau}_L)
\]
in \( Z_p \otimes_{\mathbb{Z}} (U'_L)^{1+\tau} = \lim_{\to n}( (U'_L)^{1+\tau}/p^n(U'_L)^{1+\tau}) \).

To interpret these equalities, we recall that the systems \( v(p) \) and \( c(p) \) are respectively defined to be the images of \( \tilde{v} \) and \( \tilde{c} \) under the canonical map \( \lambda : E \rightarrow E^\wedge p \). In particular, if for each \( n \) we fix an element \( x_n \) of \( R^+ \) that has the same image under the projection map \( R^+ \rightarrow \mathbb{Z}[G^+_L]/p^n \) as does \( r_p \) under the projection map \( R^+_p \rightarrow Z_p[G^+_L]/p^n = \mathbb{Z}[G^+_L]/p^n \), and we write \( \lambda_n \) for the canonical map \( E \rightarrow E/p^nE \), then \( r_p(c(p)) \) is equal to the element \( (\lambda_n(x_{n+1}))(\tilde{c}) \) of \( E^\wedge p = \lim_{\to n}(E/p^nE) \).

In terms of this notation, the equalities (9) imply that for every \( L \) in \( \Omega(p) \), the \( L \)-components \( v^{1+\tau}_L \) and \( x_{n+1}(c^{1+\tau}_L) \) of \( \tilde{v} \) and \( \tilde{x}_{n+1}(\tilde{c}) \) differ by an element of \( p^{n+1}(U'_L)^{1+\tau} \) and thus, by Lemma 2.7 below, that the systems \( \tilde{v} \) and \( \tilde{x}_{n+1}(\tilde{c}) \) themselves differ by an element of \( p^nE \).

It follows that \( \lambda_n(\tilde{v}) = \lambda_n(x_{n+1}(\tilde{c})) \) for every \( n \), and hence that there is an equality of systems

\[
v(p) = \lambda(\tilde{v}) = (\lambda_n(\tilde{v}))_n = (\lambda_n(x_{n+1}(\tilde{c})))_n = r_p(c(p)).
\]

Since this equality implies that \( v(p) \) belongs to \( R^+_p c(p) \), it therefore completes the proof of Theorem 1.6.

**Lemma 2.7.** Fix a system \( \varepsilon = (\varepsilon_L)_{L \in \Omega(p)} \) in \( E \) and a natural number \( n \) such that \( \varepsilon_L \) is divisible by \( p^{n+1} \) in \( (U'_L)^{1+\tau} \) for every \( L \). Then \( \varepsilon \) is divisible by \( p^n \) in \( E \).

**Proof.** For each \( E \) in \( \Omega(p) \), the group \( (U'_E)^{1+\tau} \) is torsion-free and so the given hypotheses imply the existence of a unique element \( y_E \) of \( (U'_E)^{1+\tau} \) with \( \varepsilon_E = y_E^{p^{n+1}} \). For the same reason, the system \( y := (y_E)_{E \in \Omega(p)} \) inherits from \( \varepsilon \) the distribution relation (2) for all \( E' \) and \( E \) in \( \Omega(p) \), and so belongs to \( ES(p)(G_m) \). The system \( y^2 = y^{1+\tau} \) therefore belongs to \( E \).

In particular, if \( p = 2 \), then, since \( \varepsilon_E = (y_E^2)^{2^n} \) for every \( E \) in \( \Omega(p) \), the system \( \varepsilon \) is equal to \( (y^2)^{2^n} \) and so is divisible by \( 2^n \) in \( E \).

Similarly, if \( p \) is odd, then one has \( \varepsilon_E^2 = (y_E^2)^{p^{n+1}} \) for every \( E \) in \( \Omega(p) \), so that the system \( \varepsilon^2 = (y^2)^{p^n} \), and hence also the system \( \varepsilon \), itself, is divisible by \( p^n \) in \( E \). \( \Box \)

**References**

[1] D. Burns, S. Seo, On circular distributions and a conjecture of Coleman, Isr. J. Math. 241 (2021) 343-393.
[2] J. H. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bull. London Math. Soc. 23 (1991) 321-350.
[3] R. Coleman, Division values in local fields, Invent. Math. 53 (1979) 91-116.
[4] R. Coleman, On an Archimedean characterization of the circular units, J. reine Angew. Math. 356 (1985) 161-173.
[5] C. Greither, Class groups of abelian fields and the main conjecture, Ann. Inst. Fourier 42 (1992) 449-499.
[6] D. S. Kubert, S. Lang, Modular Units, Grund. math. Wiss. 244, Springer-Verlag, New York, 1981.
[7] E. Matlis, The Higher Properties of R-Sequences, J. Algebra 50 (1978) 77-112.
[8] B. Mazur, K. Rubin, Kolyvagin systems, Mem. Amer. Math. Soc. 799 (2004).
[9] 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.
[10] K. Rubin, Euler systems, Annals of Math. Studies 147, Princeton Univ. Press, 2000.
[11] S. Seo, Circular Distributions and Euler Systems, J. Number Theory 88 (2001) 366-379.
[12] S. Seo, A note on circular distributions, Acta Arith. 114 (2004) 313-322.
[13] S. Seo, Circular distributions of finite order, Math. Res. Lett. 13 (2006) 1-14.
[14] S. Seo, Truncated Euler systems, J. reine angew. Math. 614 (2008), 53-71.
[15] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. Math. 108 (1978) 107-134.
[16] 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.

King’s College London, Department of Mathematics, London WC2R 2LS, U.K.
Email address: david.burns@kcl.ac.uk

King’s College London, Department of Mathematics, London WC2R 2LS, U.K.
Email address: alexandre.daoud@kcl.ac.uk

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