Compositio Mathematica **137:** 91–98, 2003.

Circular Distributions and Euler Systems, II

SOOGIL SEO
School of Mathematics, University of Minnesota, Minneapolis, MN 55455, U.S.A.
e-mail: sgseo@kias.re.kr

(Received: 1 August 2001; accepted in final form: 16 November 2001)

Abstract. The purpose of this paper is to investigate a conjecture about the universality of the circular distribution made by Robert Coleman. The algebraic property of the universal distribution is the main ingredient in studying Euler system of Kolyvagin and Rubin. We study the universality of the circular distribution by using the Iwasawa theory and the theory of the Euler systems. The conjecture is a characterization of Euler systems in the case of number field. The results here assert that Euler systems are essentially made out of cyclotomic units.

Mathematics Subject Classifications (2000). 11R27, 11R29.

Key words. circular distribution, circular units, Coleman conjecture, Iwasawa theory, Euler systems.

1. Introduction

Let n be a positive integer. Let μ_n be the set of nth roots of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mu_\infty = \cup_{n\in\mathbb{N}} \mu_n$ and $\mu_n^* = \mu_n \setminus \{1\}$, $\mu_\infty^* = \mu_\infty \setminus \{1\}$, where $\mathbb{N}$ is the set of positive integers. A Galois equivariant map f from μ_∞^* to $\overline{\mathbb{Q}}^\times$ is called a *circular distribution* if

$$\prod_{\zeta^d=\epsilon} f(\zeta) = f(\epsilon) \qquad \text{for } \epsilon \in \mu_\infty^* \text{ and } d \in \mathbb{N}.$$

By $\mathfrak{E}$ we denote the set of all circular distributions. We give a natural $R := \varprojlim \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$ module structure on $\mathfrak{E}$. Let Φ be the Galois equivariant map from μ_∞^* to $\overline{\mathbb{Q}}^\times$ defined by

$$\Phi(\zeta) = 1 - \zeta, \qquad \zeta \in \mu_\infty^*.$$

Then one can show that Φ is a circular distribution. Coleman raised a question of whether $\mathfrak{E}$ is the cyclic R-module generated by Φ. Coleman showed that the question is not true by finding some mysterious examples in $\mathfrak{E}$ but not in $R\Phi$. More precisely for any finite set of odd primes S, let ξ_S be the Galois equivariant map on μ_∞^* defined by

$$\xi_S(\zeta_n) = \begin{cases} -1, & \text{if } n \text{ is divisible by all and only those primes in } S, \\ 1, & \text{otherwise.} \end{cases}$$

Then $\xi_S \in \mathfrak{E} \setminus R\Phi$ and, hence, $\mathfrak{E} \neq R\Phi$ ([13]).

By imposing some congruence relations on $\mathfrak{E}$ such that the above examples do not satisfy, Coleman defined an R-submodule $\mathfrak{F}$ of $\mathfrak{E}$ as follows. Let $\mathfrak{F}$ be the R submodule of $\mathfrak{E}$ such that for each prime number l and $n \in \mathbb{N}, (n, l) = 1$,

$$f(\epsilon\zeta) \equiv f(\zeta) \text{ modulo primes over } (l) \quad \text{for all } \epsilon \in \mu_l^*, \zeta \in \mu_n^*.$$

Then one can see that $\Phi \in \mathfrak{F}$ and, hence, $R\Phi \subset \mathfrak{F}$. The above examples of Coleman show that $\xi_S \in \mathfrak{E} \setminus \mathfrak{F}$ as well as $\mathfrak{E} \neq \mathfrak{F}$ ([13]). We are now ready to introduce the following conjecture made by Coleman.

CONJECTURE (Coleman). $\mathfrak{F} = R\Phi$.

To approach the proof of the conjecture, we want to show that the values of $\mathfrak{F}$ and $R\Phi$ in the μ_n^* are equal for all n. We denote by $C'(n)$ the group of cyclotomic numbers of $\mathbb{Q}(\mu_n)$, i.e., $C'(n)$ is the group generated by $1-\zeta$, $\zeta \in \mu_n^*$ over the group ring $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$. Note that $R\Phi(\zeta) := \{g(\zeta) \mid g \in R\Phi, \zeta \in \mu_n^*\} = C'(n)$. Let $\mathfrak{F}(\mu_n) = \{f(\zeta) \mid f \in \mathfrak{F}, \zeta \in \mu_n\}$. In [14], we were able to show that Greenberg's conjecture implies $\mathfrak{F}(\mu_n) = C(n)$ for all $n \in \mathbb{N}$. Without Greenberg's conjecture, we can use the argument of Euler systems ([13, 14]). The following fact is due to Rubin. For each $p \nmid \phi(n)$, $\mathfrak{F}(\mu_n) \otimes \mathbb{Z}_p = C(n) \otimes \mathbb{Z}_p$.

In this paper, we extend this result to the cyclotomic $\mathbb{Z}_p$-extensions using Iwasawa theory. Let $E(n)$ be the group of global units of $\mathbb{Q}(\mu_n)$. We let $\mathfrak{E}'(n)$ be the multiplicative subgroup of $\mathbb{Q}(\mu_n)^\times$ generated by $\{f(\zeta) \mid f \in \mathfrak{E}, \zeta \in \mu_n^*\}$ and let $\mathfrak{E}(n) = \mathfrak{E}'(n) \cap E(n)$. We now state the main theorems. Notice that even if the following theorems are about $\mathfrak{E}$, the theorems are also true for $\mathfrak{F}$.

THEOREM A. *Let p be a prime number such that $(\phi(n), p) = 1$. Then $\sharp(\mathfrak{E}(\mu_{np^r})/C(np^r) \otimes \mathbb{Z}_p) = 1$ for all r and the indices $[\mathfrak{E}(np^r) : C(np^r)]$ are bounded independently of r.*

THEOREM B. *Let $f \in \mathfrak{E}$ and p be an odd prime number. Then there is a positive integer c independent of n and f, such that*

$$f(\zeta_{p^n})^c = (1-\zeta_{p^n})^{r_n} \quad \text{with } (r_n)_{n \geqslant 1} \in \varprojlim \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})].$$

NOTATIONS

$E'(n)$ = the group generated by p-units of $\mathbb{Q}(\mu_n)^\times$, $p \mid n$.
$C'(n)$ = the subgroup of $\mathbb{Q}(\mu_n)^\times$ generated by $1-\zeta$ for $\zeta \in \mu_n^*$.
$\mathfrak{E}'(n)$ = the multiplicative subgroup of $\mathbb{Q}(\mu_n)^\times$ generated by $\{f(\zeta) | f \in \mathfrak{E}, \zeta \in \mu_n^*\}$.
$E(n)$ = the group of global units of $\mathbb{Q}(\mu_n)$.
$C(n) = C'(n) \cap E(n)$, and $\mathfrak{E}(n) = \mathfrak{E}'(n) \cap E(n)$.
E_n = the group of global units of $\mathbb{Q}(\mu_n)^+$.
$\mathfrak{E}_n = \mathfrak{E}(n) \cap \mathbb{Q}(\mu_n)^+$ and $C_n = C(n) \cap \mathbb{Q}(\mu_n)^+$.

https://doi.org/10.1023/A:1023644822410 Published online by Cambridge University Press

C_n = the group of cyclotomic units of $\mathbb{Q}(\mu_n)^+$.
Cl_n = the p-part of the ideal class group of $\mathbb{Q}(\mu_n)^+$.
(We use similar notations for the $\mathfrak{F}$ i.e., $\mathfrak{F}'(n)$, $\mathfrak{F}(n)$ and $\mathfrak{F}_n$.)

2. Main Results

Let $n = n_0 p$, $(n_0, p) = 1$. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_n)^+/\mathbb{Q})$ be the Galois group of the maximal totally real subfield $\mathbb{Q}(\mu_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ of the nth cyclotomic field $\mathbb{Q}(\mu_n)$ over $\mathbb{Q}$. Let

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_\infty = \cup_{r\in\mathbb{N}} k_r = \cup_{r\in\mathbb{N}} \mathbb{Q}(\mu_{np^r})^+$$

denote the cyclotomic $\mathbb{Z}_p$-extension of $k = \mathbb{Q}(\mu_n)^+$. If $\chi\colon \Delta \longrightarrow \overline{\mathbb{Q}}_p^{\times}$ is a $\overline{\mathbb{Q}}_p^{\times}$-valued character of Δ, let $\mathbb{Q}_p(\chi)$ be the field generated by the values of χ over $\mathbb{Q}_p$. If $\chi, \psi\colon \Delta \to \overline{\mathbb{Q}}_p^{*}$ are p-adic characters, we say χ is *conjugate* to ψ over $\mathbb{Q}_p$ if there is a $\sigma \in G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\chi = \sigma\psi$. Let Ξ be the set of conjugacy classes of p-adic characters of Δ. Then each element in Ξ corresponds to an isomorphism class of an irreducible $\mathbb{Z}_p$-representation of Δ. Let $\mathbb{Z}_p(\chi)$ be the ring of integers of $\mathbb{Q}_p(\chi)$. Let M be a $\mathbb{Z}_p[\Delta]$-module. We let $M^\chi := M \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)$ be the χ-part of M where G acts via χ. Let e_χ be the idempotent of $\mathbb{Z}_p[\Delta]$ corresponding to χ,

$$e_\chi = \frac{1}{|\Delta|} \sum_{\delta\in\Delta} \mathrm{Tr}_{\mathbb{Q}_p(\chi)/\mathbb{Q}_p}\, \chi(\delta^{-1})\delta,$$

where $\mathrm{Tr}_{\mathbb{Q}_p(\chi)/\mathbb{Q}_p}$ is the trace map from $\mathbb{Q}_p(\chi)$ to $\mathbb{Q}_p$. The group ring $\mathbb{Z}_p[\Delta]$ decomposes as a product of discrete valuation rings, $\mathbb{Z}_p[\Delta] = \prod_{\chi\in\Xi} e_\chi \mathbb{Z}_p[\Delta] = \prod_{\chi\in\Xi} \mathbb{Z}_p(\chi)$, $M^\chi = e_\chi M$ and $M = \prod_{\chi\in\,\Xi} M^\chi$. For each prime $\mathfrak{p}$ of $\mathbb{Q}(\mu_{np^r})^+$ over p, let $U_\mathfrak{p}^1$ be the group of principal units in the completion $\mathbb{Q}(\mu_{np^r})_\mathfrak{p}^+$ of $\mathbb{Q}(\mu_{np^r})^+$ at $\mathfrak{p}$. For a given submodule M of E_{np^r}, let $M^1 = M \cap \prod_{\mathfrak{p}|p} U_\mathfrak{p}^1$ under the natural inclusion of M to $\mathbb{Q}(\mu_{np^r})_\mathfrak{p}^+$ and $\bar{M}$ be the topological closure of M^1 in $\prod_{\mathfrak{p}|p} U_\mathfrak{p}^1$, $M \otimes \mathbb{Z}_p \xrightarrow{\sim} \bar{M} \subset \prod_{\mathfrak{p}|p} U_\mathfrak{p}^1$. The isomorphism follows from the fact that Leopoldt conjecture is true in abelian case. Let $\bar{E}_\infty = \varprojlim \bar{E}_{np^r}$, $\bar{\mathfrak{E}}_\infty = \varprojlim \bar{\mathfrak{E}}_{np^r}$, $\bar{C}_\infty = \varprojlim \bar{C}_{np^r}$, $Cl_\infty = \varprojlim Cl_{np^r}$, with respect to the norm maps. For each finitely generated Λ-module N, the structure theorem of finitely generated Λ-modules asserts that there is a pseudo-isomorphism, $N \sim \Lambda^r \times \prod_{i\in I} \Lambda/\mathfrak{P}_i^{n_i}$, where $\mathfrak{P}_i$ are the prime ideals of height 1. We denote by $\mathrm{char}(N)$ the product of all these prime ideals $\mathfrak{P}_i$; $\mathrm{char}(N) = \prod_{i\in I} \mathfrak{P}_i^{n_i}$. In fact, since the prime ideals $\mathfrak{p}$ of height 1 in Λ are (p) and the ideals generated by an irreducible Weierstrass polynomial $F(t)$ over $\mathbb{Z}_p$, we can write

$$N \sim \Lambda^r \times \prod_{i\in I'} \Lambda/p^{m_i} \times \prod_{j\in I''} \Lambda/F_j^{n_j}.$$

Let χ be a $\mathbb{Z}_p$-valued even character of $\mathrm{Gal}(\mathbb{Q}(\mu_{np})/\mathbb{Q})$. When $k = \mathbb{Q}(\mu_p)^+$, we have Iwasawa's main conjecture $\mathrm{char}((\bar{E}_\infty/\bar{C}_\infty)^\chi) = \mathrm{char}(Cl_\infty^\chi)$. The following generalized form of Iwasawa's main conjecture was proven by Mazur and Wiles [11].

https://doi.org/10.1023/A:1023644822410 Published online by Cambridge University Press

THEOREM 2.1 (Mazur and Wiles). *Let $p \nmid \phi(n)$ then for all even irreducible $\mathbb{Z}_p$-character χ of Δ we obtain* $\mathrm{char}((\bar{E}_\infty/\bar{C}_\infty)^\chi) = \mathrm{char}(Cl_\infty^\chi)$.

The proof of Iwasawa's main conjecture was simplified by the use of Euler systems by Rubin ([12, 13]) and this was extended to the generalized form by Greither (cf. ([6]). We need the following lemma due to Coleman which is Lemma 4.1 of [14] to apply Rubin's arguments in [13]. For number fields $K \subset L$, we write $N_{L/K}$ for the norm from L to K.

LEMMA 2.2 (= Lemma 4.1 of [14]). *Let $\mathcal{J}(t)$ be the set of positive square free integers divisible only by primes $\ell \equiv 1 (\mathrm{mod}\ t)$. If F is an Abelian number field of conductor t then the function on $\mathcal{J}(t)$, $\alpha(L) = N_{\mathbb{Q}(\mu_{tL})/F(\mu_L)} f(\zeta \prod_{\ell|L} \zeta_\ell)$ is an Euler system for F for any $\zeta \in \mu_t$.*

We state a crucial theorem which shows the characteristic ideal, $\mathrm{char}(\bar{\mathfrak{E}}_\infty/\bar{C}_\infty)$ of $\bar{\mathfrak{E}}_\infty/\bar{C}_\infty$ is trivial. Thus we can see that the growth of the p-part of the quotient $\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r}$ is bounded in the $\mathbb{Z}_p$-tower.

THEOREM 2.3. *Let $p \nmid \phi(n)$.* $\mathrm{char}(\bar{\mathfrak{E}}_\infty/\bar{C}_\infty) = 1$.

Proof. Rubin's arguments in his proof of Theorem 2.3.3 in [12] together with Lemma 2.2 show that $\mathrm{char}(Cl_\infty) \mid \mathrm{char}(\bar{E}_\infty/\bar{\mathfrak{E}}_\infty)$.

Since

$$\mathrm{char}(Cl_\infty) = \mathrm{char}(\bar{E}_\infty/\bar{C}_\infty) \quad \text{(Thm 2.1)}$$

and

$$\mathrm{char}(\bar{E}_\infty/\bar{\mathfrak{E}}_\infty) \mid \mathrm{char}(\bar{E}_\infty/\bar{C}_\infty),$$

Theorem 2.3 follows. □

For a given finitely generated Λ-module N, $N \sim \Lambda^r \times \prod_{i\in I} \Lambda/p^{m_i} \times \prod_{j\in I} \Lambda/F_j^{n_j}$, the Iwasawa invariants are defined by,

$$\mathrm{rank}_\Lambda(N) = r, \quad \mu(N) = \sum_{i\in I} m_i, \quad \lambda(N) = \sum_{j\in J} n_j \deg(F_j).$$

The classical Iwasawa invariants $\lambda_p(k)$, $\mu_p(k)$, $\nu_p(k)$ are defined for the p-primary part of the ideal class groups in a $\mathbb{Z}_p$-extension of any number field k (cf. [7]). For the torsion Λ-module Cl_∞, Ferrero and Washington showed that the Iwasawa invariant $\mu_p(k) = \mu(Cl_\infty)$ of the cyclotomic $\mathbb{Z}_p$-extension k_{p^∞}/k vanishes for abelian number fields (cf. [3]). Moreover Iwasawa showed that the Iwasawa invariants $\lambda(Cl_\infty)$ and $\lambda(\bar{E}_\infty/\bar{C}_\infty)$ are equal.

Theorem 2.3 together with Ferrero and Washington's theorem tell us that the Iwasawa invariants, $\lambda(\bar{\mathfrak{E}}_\infty/\bar{C}_\infty)$ as well as $\mu(\bar{\mathfrak{E}}_\infty/\bar{C}_\infty)$ are equal to 0. This means that

https://doi.org/10.1023/A:1023644822410 Published online by Cambridge University Press

$\sharp(\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r})$ is bounded independently of r. We know the natural inclusion maps are injective (cf. [5], $H^0(G_{m,n}, \bar{C}_{np^m}) = \bar{C}_{np^n}$);

$$0 \longrightarrow \bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r} \longrightarrow \bar{\mathfrak{E}}_{np^{r+1}}/\bar{C}_{np^{r+1}}.$$

Therefore they are isomorphisms and the operator on $\bar{\mathfrak{E}}_{np^{r+k}}/\bar{C}_{np^{r+k}}$ norm to $\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r}$ followed by inclusion is the multiplication by p^k. Hence, the inverse limit of $\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r}$ with respect to the norm maps is zero; $\varprojlim(\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r}) = 1$. Let Frob_p be the Frobenius map at p, $\mathrm{Frob}_p(\zeta_u) = \zeta_u^p$ for all $(u, p) = 1$. For each element f in $\mathfrak{E}$, the sequence $(f(\zeta_{np^r}))_{r\in\mathbb{N}}$ can be made a norm coherent sequence $(\tilde{f}(\zeta_{np^r}))_{r\in\mathbb{N}} := (f(\zeta_{p^r}\zeta_n^{\mathrm{Frob}_p^{-r}}))_{r\in\mathbb{N}}$ with respect to the norm maps, $N_{\mathbb{Q}}(\mu_{np^{r+k}})/\mathbb{Q}(\mu_{np^r})$. This argument together with $\varprojlim(\bar{\mathfrak{E}}_{np^r}/\bar{C}_{np^r}) = 1$ lead to,

THEOREM 2.4. *Suppose that $p \nmid \phi(n)$. Then*

$$\sharp\left(\frac{\mathfrak{E}_{np^r}}{C_{np^r}} \otimes \mathbb{Z}_p\right) = 1, \quad \textit{for all } r.$$

As an immediate corollary we have

COROLLARY 2.5. $\sharp(\mathfrak{E}_{\mathfrak{p}^r}/\mathfrak{C}_{\mathfrak{p}^r} \otimes \mathbb{Z}_p) = 1$, *for all r.*

For a prime $l \nmid \phi(np^2)$, we consider the $\mathbb{Z}_l$-extension $\mathbb{Q}(\mu_{np^r l^\infty})$ of $\mathbb{Q}(\mu_{np^r})$. Applying Theorem 2.4, the indices $\sharp(\mathfrak{E}_{np^r l^s}/C_{np^r l^s} \otimes \mathbb{Z}_l) = 1$ for all s.

Since $H^0(G_{np^r l^s, np^r}, C_{np^r l^s} \otimes \mathbb{Z}_l) = C_{np^r} \otimes \mathbb{Z}_l$, we conclude

THEOREM 2.6. *Suppose that $l \nmid \phi(np^2)$. Then $\sharp(\mathfrak{E}_{np^r}/C_{np^r} \otimes \mathbb{Z}_l) = 1$, for all r.*

Suppose now that $l(\neq p) \mid \phi(np^2)$. To bound the l-part $\sharp(\mathfrak{E}_{np^r}/C_{np^r} \otimes \mathbb{Z}_l)$ of $\sharp(\mathfrak{E}_{np^r}/C_{np^r})$, we need the following theorem of Washington.

THEOREM 2.7 (Washington). *Let k be an Abelian number field and K/k the cyclotomic $\mathbb{Z}_p$-extension of k. Let $l \neq p$ be a prime and let l^{e_n} be the exact power of l dividing h_n. Then e_n is bounded independently of n.*

From Washington's theorem, we have that $\sharp(\mathfrak{E}_{np^r}/C_{np^r} \otimes \mathbb{Z}_l)$ is bounded independently of r. Hence, Washington's theorem and Theorem 2.6 imply that $\sharp(\mathfrak{E}_{np^r}/C_{np^r})$ is bounded independently of r. To finish the proof of Theorem A we need a lemma.

Let j be the complex conjugation. For any $\eta \in E(n)$, we have

$$\eta/\eta^j = (-\zeta_n)^a = (1-\zeta_n)^{a(1-j)}$$

for some $a \in \mathbb{Z}$, and $\eta(1-\zeta_n)^{-a}$ lies in E_n. Hence, $E(n) = E_n\mathfrak{E}(n)$. The natural map induces the following isomorphism $E(n)/\mathfrak{E}(n) \cong E_n/\mathfrak{E}_n$. Moreover, $E'(n)$ and $\mathfrak{E}(n)'$ can be written, as

https://doi.org/10.1023/A:1023644822410 Published online by Cambridge University Press

$$E'(n) = E(n) \oplus \prod_{p^{e(p)}||n} (1-\zeta_{p^{e(p)}})^{\mathbb{Z}}, \quad \text{and} \quad \mathfrak{E}(n)' = \mathfrak{E}(n) \oplus \prod_{p^{e(p)}||n} (1-\zeta_{p^{e(p)}})^{\mathbb{Z}}.$$

This provides us the proof of the following lemma.

LEMMA 2.8. *For all n,*

$$E'(n)/\mathfrak{E}(n)' \cong E(n)/\mathfrak{E}(n) \cong E_n/\mathfrak{E}_n,$$

and

$$E'(n)/\widetilde{\mathfrak{E}}(n)' \cong E(n)/\widetilde{\mathfrak{E}}(n) \cong E_n/\widetilde{\mathfrak{E}}_n.$$

Theorem 2.6 together with Lemma 2.8 complete the proof of Theorem A.

As a corollary to Theorem A, we can obtain the following theorem.

THEOREM 2.9. *For each $f \in \mathfrak{E}$, there is a constant c independent of f and s so that $f(\zeta_{p^m})^c$ can be written*

$$f(\zeta_{p^m})^c = (1-\zeta_{p^m})^{r_m}, \quad \textit{with} \ \ r_m \in \varprojlim \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q})].$$

To prove Theorem 2.9 we need to compute the annihilators of cyclotomic units in the group ring, $R_{p^m} := \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q})]$. Using this, for each norm coherent sequence $\alpha_m = (1-\zeta_{p^m})^{a(m)}$ in the p-tower, we can find representatives of $a(m)$ in $\varprojlim R_{p^m}$. For each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q})$ we denote by $\sigma = \sigma_i$ when $\sigma(\zeta_{p^m}) = \zeta_{p^m}^i$. Let $v_i := \sigma_i - \sigma_{-i}$ and let

$$w_k := \begin{cases} 4v_1 - 2v_2, & \text{when } k = 1 \\ kv_1 - v_{k_1}, & \text{when } k \neq 1. \end{cases}$$

PROPOSITION 2.10. *The annihilator $\mathcal{A}(p^m)$ of $1-\zeta_{p^m}$ in the group ring R_{p^m} is generated by the following set as $\mathbb{Z}$-module:*

$$\mathcal{S}_{p^m} = \{w_1, \ w_k \ \mid \ 3 \le k \le p^m, (k,p) = 1, \ k \textit{ odd number}\}.$$

Proof. Let φ_{p^m} be the map $\varphi_{p^m}: R_{p^m} \longrightarrow C'(p^m)$ defined by $\varphi_{p^m}(a) = (1-\zeta_{p^m})^a$ and $\overline{\varphi}_{p^m}$ be the map followed by the projection map from $C'(p^m)$ to $C'(p^m)/\mu_{p^m}$, $\overline{\varphi}_{p^m}: R_{p^m} \longrightarrow C'(p^m)/\mu_{p^m}$. Write $\mathcal{A}(p^m) = \mathrm{Ker}(\varphi_{p^m})$ for the annihilators of $(1-\zeta_{p^m})$ in R_{p^m} and $\mathcal{A}_{p^m} = \mathrm{Ker}(\overline{\varphi}_{p^m})$. Then we have the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}(p^m) & \longrightarrow & R_{p^m} & \longrightarrow & C(p^m) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{A}_{p^m} & \longrightarrow & R_{p^m} & \longrightarrow & C(p^m)/\pm\mu_{p^m} & \longrightarrow & 0 \end{array}$$

By the snake lemma we see that the cokernel of the map from $\mathcal{A}(p^m)$ to $\mathcal{A}_{p^m}$ has order $2p^m$. Now, $C(p^m)/\mu_{p^m}$ and R_{p^m} are free $\mathbb{Z}$-modules of rank $\varphi(p^m)/2$, $\varphi(p^m)$, respectively. By comparing the rank in the second row, we can see that

https://doi.org/10.1023/A:1023644822410 Published online by Cambridge University Press

$G_1 := \{v_i \mid 1 \le i \le p^m,\ (i,p)=1,\ i:\ \text{odd number}\}$ is a $\mathbb{Z}$-basis for $\mathcal{A}_{p^m}$. We also define the following $\mathbb{Z}$-independent set G_2 in $\mathcal{A}(p^m)$, $G_2 := \{w_1, w_k \mid 3 \le k \le p^m,\ (k,p)=1,\ k:\text{odd number}\}$. We let $A=(a_{ij})$ be a $\varphi(p^m)/2 \times \varphi(p^m)/2$ matrix defined in the following way: $w_i = \sum a_{ij}v_j$, where w_i and v_i are ordered as above. Then A can be written,

$$\begin{pmatrix} 4 & 0 & 0 & 0 & \cdots & 2 \\ 3 & -1 & 0 & 0 & \cdots & 0 \\ 5 & 0 & -1 & 0 & 0\cdots & 0 \\ \vdots & & & & & \\ p^m-4 & 0 & 0 & \cdots & -1 & 0 \\ p^m-2 & 0 & 0 & 0 & \cdots & -1 \end{pmatrix}$$

The absolute value of the determinant is $2p^m$ which shows that G_2 is a $\mathbb{Z}$-basis for $\mathcal{A}(p^m)$ from the above diagram. □

Proposition 2.10 tells us that we can lift each annihilators of $\mathcal{A}_{p^m}$ in p-tower.

LEMMA 2.11. *Let* $\varprojlim \mathcal{A}(p^m)$ *be the inverse limit of* $\mathcal{A}(p^m)$ *with respect to restriction maps. Then the natural projection map from* $\varprojlim \mathcal{A}(p^m)$ *to* $\mathcal{A}(p^m)$ *is surjective* $\varprojlim \mathcal{A}(p^m) \longrightarrow \mathcal{A}(p^m) \longrightarrow 0$.

Proof. Each element of the set $\mathcal{S}_{p^m}$ in Proposition 2.10 lifts to an element of the set $\mathcal{S}_{p^{m+1}}$. □

Using Lemma 2.11, we show the following proposition.

PROPOSITION 2.12. *For any* $f \in \widetilde{\mathcal{E}}$ *and prime* p, *there exist an* $r=(r_m) \in \varprojlim R_{p^m}$ *such that for all* m, $f(\zeta_{p^m}) = (1-\zeta_{p^m})^{r_m}$ *if and only if* $\widetilde{\mathcal{E}}_{p^m} = \mathcal{C}_{p^m}$ *for all* n.

Proof. Let $f(\zeta_{p^m}) = (1-\zeta_{p^m})^{u_m}$. The natural restriction map $r_{s,m}: R_{p^s} \longrightarrow R_{p^m}$ takes u_{p^s} to u_{p^m} modulo the annihilators in R_{p^m} of $1-\zeta_{p^m}$ whenever $s \ge m$ by the norm coherent property of $f(\zeta_{p^m})$. Thus $r_{s,m}(u_s) - u_m$ in $\mathcal{A}(p^m)$. This element can be lifted to get $u \in \varprojlim R_{p^m}$ by Lemma 2.11. □

From Proposition 2.12 and Theorem A, there is a constant c such that

$$f(\zeta_{p^m})^c = (1-\zeta_{p^m})^{r_m},\ \text{with } r_m \in \varprojlim R_{p^m}.$$

This completes the proof of Theorem 2.9 which is Theorem B.

Acknowledgements

I would like to thank Robert Coleman for his helpful comments. I would also like to thank Karl Rubin for the assurance and suggestion on the proof of Theorem 2.3. Finally we would like to thank the referee for helpful comments and suggestions.

References

1. Coleman, R.: Division values in local fields, *Invent. Math.* **53** (1979), 91–116.
2. Coleman, R.: On an Archimedean characterization of the circular units, *J. reine angew. Math.* **356** (1985), 161–173.
3. Ferrero, B. and Washington, L.: The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.
4. Greenberg, R.: On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.
5. Gold, R. and Kim, J.: Bases for the cyclotomic units, *Compositio Math.* **71** (1989), 13–27.
6. Greither, C.: Class groups of abelian fields, and the main conjecture, *Ann. Inst. Fourier* (*Grenoble*) **42** (1992), 449–499.
7. Iwasawa, K.: On $\mathbb{Z}_l$-extensions of algebraic number fields, *Ann. of Math.* **98** (1973), 246–326.
8. Kolyvagin, V. A.: Euler system, In: *The Grothendieck Festschrift, vol. 2*, Birkhäuser, Basel, 1990, pp. 435–483,
9. Lang, S.: *Cyclotomic Fields*, Grad. Texts in Math., Springer, New York, 1990.
10. Leopoldt, H.: Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkorper, Abh. Deutsche Akad. Wiss. Berlin Math. (1954).
11. Mazur, B. and Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.
12. Rubin, K.: The Main Conjecture, Appendix to the second edition of S. Lang: *Cyclotomic Fields*, Springer, New York, 1990.
13. Rubin, K.: *Euler Systems*, Ann of Math Stud, 147, Hermann Weyl Lectures, Princeton University Press, 2000.
14. Seo, S.: Circular distributions and Euler systems, *J. Number Theory* **88** (2001), 366–379.
15. Sinnott, W.: On the Stickelberger ideal and the circular units of a cyclotomic field, *Ann. of Math.* **108** (1978), 107–134.
16. Sinnott, W.: On the Stickelberger ideal and the circular units of an abelian field, *Invent. Math.* **62** (1980), 181–234.
17. Washington, L.: The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$ extension, *Invent. Math.* **49** (1979), 87–97.
18. Washington, L.: *Introduction to Cyclotomic Fields*, Grad. Texts in Math., Springer, New York, 1982.