ACTA ARITHMETICA
114.4 (2004)

A note on circular distributions

by

SOOGIL SEO (Seoul)

1. Introduction. Let μ_n be the set of nth roots of unity in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mu_\infty = \bigcup_{n\in\mathbb{N}} \mu_n$, $\mu_n^* = \mu_n \setminus \{1\}$, $\mu_\infty^* = \mu_\infty \setminus \{1\}$, where $\mathbb{N}$ is the set of positive integers. A *circular distribution* (cf. [1], [2]) is a Galois equivariant map f from μ_∞^* to $\overline{\mathbb{Q}}^\times$ such that

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

We denote by Σ the set of all circular distributions. Let

$$R_n := \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})]$$

be the group ring of the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ and $R := \varprojlim R_n$ be the projective limit of R_n with respect to the natural restriction maps. Then Σ has a natural R-module structure. Let ψ be the element of Σ defined by

$$\psi(\zeta) = 1 - \zeta, \quad \zeta \in \mu_\infty^*.$$

By finding elements in Σ but not in $R\psi$, Coleman checked that $\Sigma \neq R\psi$. He defined a subgroup $\mathcal{F}$ of Σ consisting of $f \in \Sigma$ satisfying, for each prime number l and $n \in \mathbb{N}$ with $(l,n) = 1$,

$$f(\varepsilon\zeta) \equiv f(\zeta) \quad \text{modulo primes over } (l)$$

for all $\varepsilon \in \mu_l^*, \zeta \in \mu_n^*$. Coleman conjectured

CONJECTURE (Coleman). *$\mathcal{F} = R\psi$.*

In [11], by using the Iwasawa theory (cf. [5]) and arguments involving Euler systems (cf. [6], [8] and [9]) we showed that the values of $\mathcal{F}$ and $R\psi$ on μ_n^* are "essentially" equal for all n. In [10], we were able to show that Greenberg's conjecture implies that the values of $\mathcal{F}$ and $R\psi$ on μ_n^* are equal for all n. In this paper we investigate to what extent the equality of

2000 *Mathematics Subject Classification*: 11R27, 11R29.
Key words and phrases: circular distribution, circular units, Coleman conjecture, Iwasawa theory.

values of $\mathcal{F}$ and $R\psi$ implies Coleman's conjecture. Let $C(n)$ be the group of Sinnott's cyclotomic units in the field $\mathbb{Q}(\mu_n)$ (cf. [12], [13]),

$$C(n) := \{(1-\zeta)^r \mid \zeta \in \mu_n,\, r \in R\}.$$

Note that the set of values of $R\psi$ on μ_n^* is $C(n)$. Hence throughout this paper we will assume that $\mathcal{F}(\mu_n) = C(n)$ for all n. For each $n \in \mathbb{N}$, let ζ_n be a primitive nth root of unity in μ_n such that $\zeta_{mn}^m = \zeta_n$ for all $m, n \in \mathbb{N}$. Let $D(n)$ be the R-submodule of $C(n)$ generated by $1-\zeta_n$. We prove

THEOREM A. *Let $f \in \mathcal{F}$. Then $f(\zeta_n) \in D(n)$ for all $n \in \mathbb{N}$.*

We first show that $\mathcal{F}(\zeta_n)$ is a cyclic R_n-module. Let $n = p_1^{e_1} \cdots p_r^{e_r}$. Let E_n denote the group of global units of the nth cyclotomic field and $C_n := C(n) \cap E_n$. In general C_n is generated as an R-module by

$$\{1-\zeta_t \mid t \,\|\, n,\ t \text{ is divisible by at least two distinct primes}\} \cup \left\{ \frac{1-\zeta_{p_i^{e_i}}^{a_i}}{1-\zeta_{p_i^{e_i}}} \,\middle|\, i = 1, \ldots, r \right\},$$

which is a set of cardinality $\sum_{i=2}^r \binom{r}{i} + r = \sum_{i=1}^r \binom{r}{i} = 2^r - 1$. Then we use a basis for C_n modulo $\pm\mu_n$ constructed by M. Conrad (see §2).

In Section 3, we compute the torsion subgroups Σ_{tor} and $\mathcal{F}_{\mathrm{tor}}$ of Σ and $\mathcal{F}$ respectively. For any set S of square free odd numbers, let δ_S be the function on μ_∞^* defined by

$$\delta_S(\zeta_n) = \begin{cases} -1 & \text{if } n \text{ involves only primes in } S, \\ 1 & \text{otherwise.} \end{cases}$$

Let $\mathcal{D}$ be the R-submodule of Σ generated by δ_S for all such S. When S is the set of all square free odd numbers, we denote δ_S by δ_{odd}. We prove

THEOREM B. $\Sigma_{\mathrm{tor}} = \mathcal{D}$, $\mathcal{F}_{\mathrm{tor}} = \langle \delta_{\mathrm{odd}} \rangle$.

Acknowledgements. We would like to thank Robert Coleman for his helpful comments and suggestions. We also would like to thank Sung Han Bae for his helpful comments and suggestions on the first draft. Finally, we thank School of Mathematics, KIAS for research support.

2. $\mathcal{F}(\zeta_n)$ is cyclic. Let $\widehat{\mathbb{Z}}$ be the profinite group $\varprojlim(\mathbb{Z}/n\mathbb{Z}) = \prod_p \mathbb{Z}_p$. Let $\chi : \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \to \mathrm{Aut}(\mu_\infty) = \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ be the cyclotomic character defined by $\zeta^\sigma = \zeta^{\chi(\sigma)}$ for all $\zeta \in \mu_\infty$. Recall that

$$\Sigma := \left\{ f : \mu_\infty^* \to \overline{\mathbb{Q}}^\times \,\middle|\, \begin{array}{l} \bullet\ \prod_{\zeta^d = \varepsilon} f(\zeta) = f(\varepsilon) \text{ for } \varepsilon \in \mu_\infty^* \text{ and } d \in \mathbb{N}, \\ \bullet\ \sigma(f(\zeta)) = f(\zeta^{\chi(\sigma)}) \text{ for } \sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \end{array} \right\}$$

and

$$\mathcal{F} := \left\{ f \in \Sigma \;\middle|\; \begin{array}{l} \text{for each prime number } l \text{ and } n \in \mathbb{N} \text{ with } (l,n)=1, \\ f(\varepsilon\zeta) \equiv f(\zeta) \text{ modulo primes over } (l) \text{ for all } \varepsilon \in \mu_l^*, \zeta \in \mu_n^* \end{array} \right\}.$$

Let $\mathcal{F}(\zeta_n) := \{f(\zeta_n) \mid f \in \mathcal{F}\}$ and $\mathcal{F}_n := \mathcal{F}(\zeta_n) \cap E_n$, where E_n is the group of units in $\mathbb{Q}(\mu_n)$. Let $C(n)$ be the group of circular numbers of the nth cyclotomic field $\mathbb{Q}(\mu_n)$, as defined above, and C_n the group of circular units (in the sense of Sinnott [12]),

$$C_n := C(n) \cap E_n.$$

It follows from

$$\frac{\mathcal{F}(\mu_n)}{C(n)} \cong \frac{\mathcal{F}_n}{C_n} \quad \text{for all } n \in \mathbb{N}$$

that we can transform results on $\mathcal{F}(\zeta_n), C(n)$ into those on $\mathcal{F}_n, C_n$ and vice versa. Furthermore the fact (cf. [10]) that if n is divisible by two distinct primes then $f(\zeta_n)$ is always a unit allows us to supress the distinction whether $f(\zeta_n)$ lies in $C(n)$ or C_n.

Let $n = p_1^{e_1} \cdots p_r^{e_r}$. For each p_i we choose $a_i \in \mathbb{N}$ such that a_i generates $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ as a multiplicative group. If $p_i = 2$ then we assume $e_i \geq 2$, $(\mathbb{Z}/2^{e_i}\mathbb{Z})^\times = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e_i-2}\mathbb{Z}$ and choose a generator a_i of $\mathbb{Z}/2^{e_i-2}\mathbb{Z}$. Write $a \,\|\, b$ when a divides b and a is prime to b/a. In general, C_n is generated as an R-module by

$$\{1 - \zeta_t \mid t \,\|\, n,\ t \text{ is divisible by at least two distinct primes}\}$$
$$\cup \left\{ \frac{1 - \zeta_{p_i^{e_i}}^{a_i}}{1 - \zeta_{p_i^{e_i}}} \;\middle|\; i = 1, \ldots, r \right\},$$

which is a set of cardinality $\sum_{i=2}^r \binom{r}{i} + r = \sum_{i=1}^r \binom{r}{i} = 2^r - 1$. Finding a minimal set of generators over R depends heavily on the prime factors of n (cf. [4]). For instance if $n = pq$, p generates $\mathbb{Z}/q\mathbb{Z}$ and q generates $\mathbb{Z}/p\mathbb{Z}$ then one sees easily that $C_{pq} = R(1 - \zeta_{pq})$; $p = 3$, $q = 5$ will satisfy this condition. On the other hand, $C_{55} \neq R(1 - \zeta_{55})$ as C_5 is not contained in $R(1 - \zeta_{55})$.

Now, we want to show that $\mathcal{F}(\zeta_n)$ is a cyclic R_n-module generated by $1 - \zeta_n$. For $n \mid m$ we let

$$s_{m,n} := \Big(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_n))} \sigma \Big) \in R_m$$

and denote the norm map from $\mathbb{Q}(\mu_m)$ to $\mathbb{Q}(\mu_n)$ by $N_{m,n}$.

For motivation, let us consider the case $n = p^r q$ where p and q are distinct primes. For $f \in \mathcal{F}$, if $f(\zeta_{p^r q}) \in C(p^r q)$ then it follows from the formula

$$(1 - \zeta_{p^r}\zeta_q)^{s_{p^r q, p^{r-1} q}} = (1 - \zeta_{p^{r-1}}\zeta_q^p)$$

that $f(\zeta_{p^r}\zeta_q^{p^{-(r-1)}})$ can be expressed in the following form:

$$f(\zeta_{p^r}\zeta_q^{p^{-(r-1)}}) = (1-\zeta_{p^r}\zeta_q^{p^{-(r-1)}})^{a_r}(1-\zeta_{p^r})^{b_r}(1-\zeta_q)^{c_r}, \tag{1}$$

for some $a_r, b_r, c_r \in R_{p^rq}$. The product condition

$$\prod_{\zeta^d=\varepsilon} f(\zeta) = f(\varepsilon)$$

for $\varepsilon \in \mu_\infty$ and $d \in \mathbb{N}$ is known to be equivalent to the following conditions (see Section 2 of [10]):

- For any prime number l and square free integer r with $(r,l)=1$,

$$N_{lr,r} f(\zeta_l\zeta_r) = f(\zeta_r)^{\mathrm{Fr}_l - 1} \quad \text{if } r \neq 1.$$

- For $n-i \geq 1$,

$$N_{l^nr,l^{n-1}r} f(\zeta_{l^n}\zeta_r^i) = f(\zeta_{l^{n-i}}\zeta_r^l).$$

Here Fr_p is Frobenius at p. It then follows from $N_{p^rq,pq} f(\zeta_{p^r}\zeta_q^{p^{-(r-1)}}) = f(\zeta_p\zeta_q)$ and (1) that

$$(1-\zeta_p\zeta_q)^{a_r}(1-\zeta_p)^{b_r}((1-\zeta_q)^{c_r})^{p^{r-1}} = (1-\zeta_p\zeta_q)^{a_1}(1-\zeta_p)^{b_1}(1-\zeta_q)^{c_1}$$

for all $n \geq 1$. Even if the exponent p^{r-1} in the last term on the left hand side is large, it may be compensated for by the first term as

$$(1-\zeta_{pq})^{s_{pq,q}} = (1-\zeta_q)^{\mathrm{Fr}_p - 1}.$$

This problem occurs because $(1-\zeta_{p^rq})^{R_{p^rq}}$ and $(1-\zeta_q)^{R_q}$ are not necessarily linearly disjoint over $\mathbb{Z}$,

$$1 \neq (1-\zeta_{p^rq})^{s(p^rq,q)R_{p^rq}} = (1-\zeta_q)^{(\mathrm{Fr}_p-1)R_q} \subset (1-\zeta_{p^rq})^{R_{p^rq}} \cap (1-\zeta_q)^{R_q}.$$

With this regard, the expression of (1) seems to be possible without $(1-\zeta_q)^{c_r}$ equaling 1. We will show this is not the case.

We mention here that the study of inverse limits of circular units was considered in a long and interesting paper [7] of Kuz'min. In the first section of [7], Kuz'min finds a set of generators for $\overline{P}_\infty$, the inverse limit of $\overline{P}_n$, the circular units modulo roots of unity over the cyclotomic $\mathbb{Z}_p$ extension. He presents $\overline{P}_n$ as a product of D_n and P_{-1} in order to obtain the inverse limit of $\overline{P}_n$ as that of D_n. We show that the inverse limit of $\overline{P}_n$ can be obtained only in terms of D_n independently of P_{-1} using a nice basis found by Conrad. This basis behaves well with respect to the norm maps in the cyclotomic $\mathbb{Z}_p$ extension.

Conrad constructed a basis B_n for the group of cyclotomic units (modulo $\pm\mu_n$) of the nth cyclotomic field. (The "modulo $\pm\mu_n$" does not concern us since $-\zeta_n = (1-\zeta_n)^{1-\tau}$ for the complex conjugation τ.) The *relative circular* *units* $\widehat{C}_n$ are defined to be the group

$$\frac{C_n}{\pm\mu_n \prod_{d\mid n,\, d\neq n} C_d}.$$

THEOREM 2.1. *If $\widehat{B}_d \subset C_d$ maps to a basis of $\widehat{C}_d$ for $d\mid n$ then $B_n = \bigcup_{d\mid n} \widehat{B}_d$ maps to a basis of $C_n/(\pm\mu_n)$.*

Proof. See Theorem 5.3 of [3]. ∎

Indeed, Conrad constructed a basis $B_n = \bigcup_{d\mid n} \widehat{B}_d$ of C_n so that $\widehat{B}_d$ induces a basis for the group of relative cyclotomic units $\widehat{C}_d$ ([3, pp. 13, 14]). In what follows by $\widehat{B}_d \subset C_d$ we denote a subset of C_d which maps to a basis of $\widehat{C}_d$. Let $D(n)$ be the cyclic R_n-module generated by $1-\zeta_n$ and D_n be the units in $D(n)$,

$$D(n) := (1-\zeta_n)^{R_n} = \{(1-\zeta_n)^{r_n} \mid r_n \in R_n\}, \qquad D_n := D(n) \cap E_n.$$

Note that $D(n) = D_n$ if n is divisible by two distinct primes. Let $n = p_1^{e_1}\cdots p_r^{e_r}$. It follows from the observation

$$D(p_1^{a_1}\cdots p_r^{a_r}) \subset D(p_1^{b_1}\cdots p_r^{b_r}) \quad \text{for } 1 \le a_i \le b_i$$

that $C_n = \prod_{d\|n} D_d$. It also follows that

$$\widehat{C}_n = \frac{\prod_{a\|n} D_a}{\prod_{d\mid n,\, d\neq n}\prod_{b\|d} D_b} \approx \frac{D_n}{\prod_{n'\mid n,\, p_1\cdots p_r\mid n'} D_{n'}}.$$

From this we are led to the following

LEMMA 2.2. *Let $b \in \widehat{B}_n$. Then we can write $b = (1-\zeta_n)^{r_n}$ for some $r_n \in R_n$.*

Let $\langle \widehat{B}_d\rangle$ denote the group generated by $\widehat{B}_d$.

LEMMA 2.3. $N_{p^w f, p^v f}(\langle \widehat{B}_{p^w f}\rangle) = \langle \widehat{B}_{p^v f}\rangle$ *for* $1 \le v \le w$.

Proof. The norm map $N_{p^w f, p^v f}$ induces a surjective map from $\widehat{C}_{p^w f}$ to $\widehat{C}_{p^v f}$:

$$\begin{array}{ccccc} D_{p^w f} & \xrightarrow{N_{p^w f, p^v f}} & D_{p^v f} & \longrightarrow & 0 \\ \big\downarrow & & \big\downarrow & & \\ \widehat{C}_{p^w f} & \xrightarrow{N_{p^w f, p^v f}} & \widehat{C}_{p^v f} & \longrightarrow & 0. \end{array}$$ ∎

THEOREM 2.4 (= Theorem A). *Let $f \in \mathcal{F}$. Then $f(\zeta_n) \in C(n)$ if and only if $f(\zeta_n) = (1-\zeta_n)^{r_n}$ for some $r_n \in R_n$.*

Proof. The “if” direction is clear, now we take care of the “only if” direction. If n is a prime power then it follows immediately from the hypotheses that $f(\zeta_n) = (1-\zeta_n)^{r_n}$. Now suppose n is divisible by two distinct primes. We know that in this case $f(\zeta_n)$ is a unit and hence $f(\zeta_n)$ lies in the group of circular units, C_n. Let $n = p_1^{e_1}\cdots p_r^{e_r}$. Let $f(\zeta_n) = \prod_{n'|n} G(n') \bmod \pm\mu_n$ for some $G(n') \in \langle \widehat{B}_{n'}\rangle$. We claim that all the $G(n')$ terms with $p_1\cdots p_r \nmid n'$ are trivial. Suppose $p \,|\, n$ and write

$$f(\zeta_n) = \prod_{p|a|n} G(a) \prod_{p\nmid b|n} G(b) \bmod \pm\mu_n.$$

Suppose $w \in \mathbb{N}$ and write

$$f(\zeta_{np^w}) = \prod_{i=1}^{w+e_1} \prod_{d|\frac{n}{p^{e_1}}} G'(p^i d) \prod_{p\nmid b} G'(b) \bmod \pm\mu_{np^w}.$$

Applying $N_{np^w,n}$ and using Lemma 2.3 we see that

$$f(\zeta_n) = \prod_{p|a} G''(a)\Big(\prod_{p\nmid b} G'(b)\Big)^{p^w} \bmod \pm\mu_n,$$

for some $G''(a) \in \langle \widehat{B}_a\rangle$. From this and Theorem 2.1 it follows that $\prod_{p\nmid b|n} G(b) \in \pm\mu_n$. Thus our claim is proved and hence

$$f(\zeta_n) = \prod G(n'),$$

where the product is taken over $n' \,|\, n$ where $p_1\cdots p_r \,|\, n'$. It then follows from Lemma 2.2 and the facts that

$$G(n') \in \langle \widehat{B}_n\rangle \quad \text{for all } n' \text{ with } p_2\cdots p_r \,|\, n'$$

and that $\pm\mu_n \subset D_n$ that

$$f(\zeta_n) = (1-\zeta_n)^{r_n} \quad \text{for some } r_n \in R_n. \ \blacksquare$$

Let $\mathcal{A}_n$ be the annihilator of D_n in R_n,

$$\mathcal{A}_n := \{r_n \in R_n \mid u^{r_n} = 1 \text{ for all } u \in D_n\}.$$

One can obtain a well defined restriction map $\mathrm{res}_{p^m a,p^n a}$ from $\mathcal{A}_{p^m a}$ into $\mathcal{A}_{p^n a}$ ($m \ge n \ge 1$) using the norm maps $N_{p^m a,p^n a}$; then $\mathrm{res}_{p^m a,p^n a}\mathcal{A}_{p^m a} \subset \mathcal{A}_{p^n a}$ and hence we have a well defined map

$$\mathrm{res}_{p^m a,p^n a} : R_{p^m a}/\mathcal{A}_{p^m a} \to R_{p^n a}/\mathcal{A}_{p^n a}.$$

From Theorem 2.4 we have

Corollary 2.5. *Let $f \in \mathcal{F}$. Then $f(\zeta_{p^n a}) \in C_{p^n a}$ if and only if $f(\zeta_{p^n a}) = (1-\zeta_{p^n a})^{r_{p^n a}}$ for some $(r_{p^n a}) \in \varprojlim(R_{p^n a}/\mathcal{A}_{p^n a})$.*

By taking inverse limits with respect to the restriction maps the short exact sequence,

$$1 \to \mathcal{A}_{p^n a} \to R_{p^n a} \to R_{p^n a}/\mathcal{A}_{p^n a} \to 1$$

produces the left short exact sequence

$$1 \to \varprojlim \mathcal{A}_{p^n a} \to \varprojlim R_{p^n a} \to \varprojlim R_{p^n a}/\mathcal{A}_{p^n a}.$$

In general $\mathcal{A}_\infty := \varprojlim \mathcal{A}_{p^n a}$ is not zero. When $a = 1$, we have $\mathcal{A}_\infty \neq 1$ for all prime p and

$$1 \to \varprojlim \mathcal{A}_{p^n} \to \varprojlim R_{p^n} \to \varprojlim R_{p^n}/\mathcal{A}_{p^n} \to 1.$$

This implies that in Corollary 2.5 we can lift elements $(r_{p^n}) \in \varprojlim(R_{p^n}/\mathcal{A}_{p^n})$ to $(r_{p^n}) \in \varprojlim R_{p^n}$. We refer to [10] for the details.

3. Σ_{tor} and $\mathcal{F}_{\mathrm{tor}}$. In this section, we will compute the torsion subgroups $\Sigma_{\mathrm{tor}}, \mathcal{F}_{\mathrm{tor}}$ of Σ and $\mathcal{F}$ respectively. We begin by considering interesting examples found by Coleman. For any set S of square free odd numbers, let δ_S be the function on μ_∞^* defined by

$$\delta_S(\zeta_n) = \begin{cases} -1 & \text{if } n \text{ involves only primes in } S, \\ 1 & \text{otherwise.} \end{cases}$$

Then one can easily check that $\delta_S \in \Sigma \setminus \mathcal{F}$ and $\delta_S^2 = 1$. Conversely, we can characterize Coleman's examples to be those $f \in \Sigma$ such that $f^2 = 1$. Indeed suppose that $f \in \Sigma, f^2 = 1$. Thus $f(\zeta_n) = \pm 1$ for any $\zeta_n \in \mu_\infty^*$. We take

$$S = \{m \mid m \text{ is square free and } f(\zeta_m) = -1\}.$$

If S is an empty set then $f = 1$ from the definition of the circular distribution. Let $n \in S$ and $n = p_1 \cdots p_r$. If n is even, say $p_1 = 2$, then f does not satisfy the axiomatic definition of circular distribution: Let $w = p_1^2 p_2 \cdots p_r, v = p_1 \cdots p_r$. Then

$$1 = (-1)^2 = N_{w,v} f(\zeta_w) = f(\zeta_v) = -1.$$

Hence the set S consists of odd numbers. We now claim that $f = \delta_S$. By the definition of δ_S and the distributive property of f we have

$$f(\zeta_n) = \delta_S(\zeta_n) = \begin{cases} -1 & \text{if } n = q_1^{e_1} \cdots q_g^{e_g} \text{ with } e_i \geq 1 \text{ for } 1 \leq i \leq r \\ & \quad \text{and } q_1 \cdots q_g \in S, \\ 1 & \text{otherwise.} \end{cases}$$

This shows that $f = \delta_S$. Let $\mathcal{D}$ be the R-submodule of Σ generated by δ_S for all such S. We obtain the following

LEMMA 3.1 (Coleman). *$\mathcal{D}$ is the submodule of Σ consisting of all elements f such that $f^2 = 1$.*

The above lemma provides us the subgroup $\mathcal{D}$ of 2-torsions of Σ. First we will show that $\mathcal{D}$ is the torsion subgroup of Σ. We fix some notations. Let $\{p_1, \ldots, p_r\}$ be a set of (temporarily fixed) distinct primes and $P := p_1 \cdots p_r$.

Let $X = X(P)$ denote the set of all numbers divisible only by P,

$$X := \{p_1^{c_1} \cdots p_r^{c_r} \mid c_i \geq 1 \text{ for all } i = 1, \dots, r\}.$$

Let

$$X_i := \{p_1 \cdots p_i^{c_i} \cdots p_r \mid c_i \geq 1\} \subset X.$$

For any subset T of $\mathbb{N}$ and $f \in \Sigma$, let

$$T(f) := \{f(\zeta_t) \mid t \in T \subset \mathbb{N}\}$$

and let $\mathbb{Q}(T(f)) := \mathbb{Q}(\alpha \mid \alpha \in T(f))$. For each $m \geq n$, we write

$$d_n^m(f) := [\mathbb{Q}(f(\zeta_m)) : \mathbb{Q}(f(\zeta_n))] \in \mathbb{N}, \quad d^T(f) := [\mathbb{Q}(T(f)) : \mathbb{Q}] \in \mathbb{N} \cup \{\infty\}.$$

We start with the following

PROPOSITION 3.2. *Suppose that $f \in \Sigma$. Then $X(f)$ is contained in $\{\pm 1\}$ if and only if $d^X(f)$ is finite. Moreover $X_i(f)$ is not contained in $\pm\mu_{P/p_i}$ if and only if $d_{Pp_i^n}^{Pp_i^{n+1}}(f)$ is equal to p_i for all sufficiently large n.*

Proof. Suppose that $d^X(f)$ is finite. Then there are positive integers $e_1, \dots, e_r$ such that $\mathbb{Q}(X(f)) \subset \mathbb{Q}(\mu_{p_1^{e_1} \cdots p_r^{e_r}})$. For any s and $n_j > e_j$ such that $s \equiv 1 \bmod p_j^{n_j}$ for $j = 1, \dots, i-1, i+1, \dots, r$, we have $f(\zeta_a) = N_{p_i^s a, a} f(\zeta_{p_i^s a}) = f(\zeta_{p_i^s a})^{p_i^s}$ where $a = p_1^{n_1} \cdots p_r^{n_r}$. As s can be made arbitrarily large, it follows that $f(\zeta_a) \in \pm\mu_{a/p_i^{n_i}}$ and hence

$$f(\zeta_a) \in \bigcap_{i=1,\dots,r} \pm\mu_{a/p_i^{n_i}} \subset \{\pm 1\}.$$

By the norm coherence property, we conclude $X(f) \subset \{\pm 1\}$. Conversely, if $X(f) \subset \{\pm 1\}$ then clearly $d^X(f)$ is finite.

If $d_{Pp_i^n}^{Pp_i^{n+1}}(f)$ is equal to p_i for all sufficiently large n then $X_i(f)$ is not contained in any finite set and hence not contained in $\pm\mu_{P/p_i}$. To prove necessity suppose that $d_{Pp_i^n}^{Pp_i^{n+1}}(f) \neq p$ for infinitely many n. Then there are infinite sequences of numbers, $n_1 < n_2 < \cdots$, and $s_1 < s_2 < \cdots$, such that $d_{Pp_i^{n_j}}^{Pp_i^{n_j+1}}(f) = 1$, $s_k \equiv 1 \bmod p_g$ for $g = 1, \dots, i-1, i+1, \dots, r$ and $s_{k-1} < n_k < s_k$. It follows from

$$f(\zeta_{Pp_i^{s_k}}) = (N_{Pp_i^{n_{k+1}}, Pp_i^{s_k}} N_{Pp_i^{s_{k+1}}, Pp_i^{n_{k+1}+1}} f(\zeta_{Pp_i^{s_{k+1}}}))^p$$

that

$$f(\zeta_{Pp_i^{s_1}}) = N_{Pp_i^{s_t}, Pp_i^{s_1}} f(\zeta_{Pp_i^{s_t}}) = \prod_{k=2,3,\dots,t} (N_{Pp_i^{n_k}, Pp_i^{s_{k-1}}} N_{Pp_i^{s_k}, Pp_i^{n_k+1}} f(\zeta_{Pp_i^{s_t}}))^{p_i^t}.$$

This leads to the conclusion that $X_i(f) \subset \pm\mu_{P/p_i}$. ∎

In the following corollary we assume that P is prime.

Corollary 3.3. *Let $P = p$ be prime. Suppose $f \in \mathcal{F}$. Then $d^X(f) \notin \{\pm 1\}$ if and only if $d^X(f) = \infty$. Moreover, in this case $d_{p^n}^{p^{n+1}}(f) = p$ for all sufficiently large n.*

Proof. This follows immediately from Proposition 3.2. ∎

Corollary 3.4. $\Sigma_{\mathrm{tor}} = \mathcal{D}$.

Proof. Apply Lemma 3.1 and Proposition 3.2. ∎

The following example which is contained in Coleman's examples of $\mathcal{D}$ was suggested to us by Bae.

Example.

$$\delta_{\mathrm{odd}}(\zeta_n) = \begin{cases} -1 & \text{if } n \text{ is odd,} \\ 1 & \text{otherwise.} \end{cases}$$

Then $\delta_{\mathrm{odd}} \in \mathcal{F}$. We will show that it generates the torsion subgroup $\mathcal{F}_{\mathrm{tor}}$ of $\mathcal{F}$.

Theorem 3.5 (= Theorem B). $\mathcal{F}_{\mathrm{tor}} = \{1, \delta_{\mathrm{odd}}\}$.

Proof. By Corollary 3.4, $\mathcal{F}_{\mathrm{tor}}$ is contained in $\mathcal{D}$, $\mathcal{F}_{\mathrm{tor}} \subset \Sigma_{\mathrm{tor}} = \mathcal{D}$. Suppose that $1 \neq f \in \mathcal{D} \cap \mathcal{F}$. Thus $f = \delta_S$ for some nonempty set S. We claim that $f = \delta_{\mathrm{odd}}$. Let $n \in S$ and $n = p_1 \cdots p_r$. Let $t \neq n$ be a square free odd number. Let q be a prime such that $(q, n) = 1, q \mid t$. It follows from the congruence conditions of $\mathcal{F}$ that

$$-1 = f(\zeta_{p_1 \cdots p_r}) \equiv f(\zeta_{qp_1 \cdots p_r}) \quad \text{modulo primes over } q.$$

Since q is an odd prime we have $f(\zeta_{qp_1 \cdots p_r}) = -1$. In this way one can easily arrive at $f(\zeta_t) = -1$. It follows from the norm coherence property that $f(\zeta_s) = -1$ for all odd numbers s as we wanted to show. ∎

We will show elsewhere that δ_{odd} can be written in the form $\delta_{\mathrm{odd}}(\zeta_n) = (1 - \zeta_n)^{r_n}$ for all n, but is not contained in $R\psi$. We are led to the question, an affirmative answer to which would be a slight modification of Coleman's original conjecture on the circular distributions:

$$\text{Does } \mathcal{F} \text{ equal } R\psi \oplus \mathcal{F}_{\mathrm{tor}}\ ?$$

References

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

[2] —, *On an Archimedean characterization of the circular units*, J. Reine Angew. Math. 356 (1985), 161–173.

[3] M. Conrad, *Construction of bases for the group of cyclotomic units*, J. Number Theory 81 (2000), 1–15.

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

[5] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. 98 (1973), 246–326.

[6] V. A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, Vol. 2, Birkhäuser, 1990, 435–483.

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

[8] K. Rubin, *The main conjecture*, Appendix to the second edition of S. Lang: *Cyclotomic Fields*, Springer, 1990.

[9] —, *Euler Systems*, Ann. of Math. Stud. 147, Princeton Univ. Press, 2000.

[10] S. Seo, *Circular distribution and Euler systems*, J. Number Theory 88 (2001), 366–379.

[11] —, *Circular distribution and Euler systems II*, Compositio Math. 137 (2003), 91–98.

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

[13] —, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.

School of Mathematics
Korea Institute for Advanced Study (KIAS)
207-43 Cheongryangri-2dong
Dongdaemun-gu
Seoul 130-722, Republic of Korea
E-mail: sgseo@kias.re.kr

Received on 6.11.2002
and in revised form on 17.3.2004 (4401)