J. Math. Soc. Japan
Vol. 37, No. 1, 1985

On cyclotomic units connected with p-adic characters

By Tsuyoshi UEHARA

(Received Aug. 23, 1983)
(Revised Dec. 8, 1983)

§ 1. Introduction.

Let p be an odd prime and let K be an abelian number field of degree prime to p which contains a primitive p-th root of unity. We denote by η_{ϕ} a ϕ-relative cyclotomic unit in the sense of Gras [2], where ϕ is a non-trivial even p-adic character of the Galois group of K over the rationals. Gras has given some congruences concerning η_{ϕ} and Bernoulli numbers associated with the reflection $\bar{\phi}$ of ϕ. Let $A(\phi)$, $A(\bar{\phi})$ be p-subgroups of the ideal class group of K corresponding to ϕ, $\bar{\phi}$ respectively. A close relation between $A(\phi)$ and $A(\bar{\phi})$ was stated by Leopoldt [5]. Recently Wiles [8] proved that if K is the p-th cyclotomic field and η_{ϕ} is a p-th power in K then $A(\phi)$ is non-trivial.

In this paper we shall give a relation between η_{ϕ} and $A(\bar{\phi})$. Namely we state a necessary and sufficient condition for η_{ϕ} to be a p-th power in K in terms of the ideals representing classes in $A(\bar{\phi})$. In the case that K is the p-th cyclotomic field, Iwasawa has shown the above result applying a theorem of Artin-Hasse concerning power residue symbols (cf. [3], Lemma 3). On the other hand our proof is essentially based on the prime factorization of certain Jacobi sums.

§ 2. Notation and results.

Throughout this paper we denote by p an odd prime and by $\boldsymbol{Z}$, $\boldsymbol{Z}_p$, $\boldsymbol{Q}$, and $\boldsymbol{Q}_p$ the ring of rational integers, the ring of p-adic integers, the field of rational numbers, and the field of p-adic numbers respectively. Further it is assumed that all integers and all algebraic number fields are contained in an algebraic closure $\bar{\boldsymbol{Q}}_p$ of $\boldsymbol{Q}_p$. For a rational integer $m>0$ let ζ_m be a primitive m-th root of unity.

Let K be an abelian number field and let χ be a character of the Galois group $\mathrm{Gal}(K/\boldsymbol{Q})$. By $g(\chi)$ we always mean the order of χ. Let K_{χ} be the fixed field of the kernel of χ. Then K_{χ} is a cyclic extension of $\boldsymbol{Q}$ of degree $g(\chi)$.

This research was partially supported by Grant-in-Aid for Scientific Research (No. 58540115), Ministry of Education.

For any abelian number field M containing K_χ we regard χ as a character of $\mathrm{Gal}(M/\boldsymbol{Q})$ by putting $\chi(\sigma)=\chi(\sigma_K)$ for each σ in $\mathrm{Gal}(M/\boldsymbol{Q})$, where σ_K is an automorphism of K whose restriction to K_χ coincides with that of σ. If K_χ is contained in $\boldsymbol{Q}(\zeta_f)$ for some $f>0$, then we identify χ and the corresponding Dirichlet character modulo f so that $\chi(a)=\chi(\sigma_a)$ for every a in $\boldsymbol{Z}$, prime to f, where σ_a is the automorphism of $\boldsymbol{Q}(\zeta_f)$ determined by $\zeta_f^{\sigma_a}=\zeta_f^a$. Let $f(\chi)$ be the least rational integer $f>0$ such that $K_\chi\subset\boldsymbol{Q}(\zeta_f)$. Then χ is a primitive Dirichlet character modulo $f(\chi)$.

Let $\boldsymbol{Q}_p(\chi)$ be the field generated by the values of χ over $\boldsymbol{Q}_p$. We introduce a p-adic character ϕ such that

$$\phi=\sum_{\tau\in H}\chi^\tau$$

with $H=\mathrm{Gal}(\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p)$, where χ^τ is a character defined by $\chi^\tau(\sigma)=\chi(\sigma)^\tau$ for any σ in $\mathrm{Gal}(K/\boldsymbol{Q})$. We call ϕ the p-adic character over χ. We put

$$e(\phi)=g(\chi)^{-1}\sum_{\sigma\in G_\chi}\phi(\sigma)\sigma^{-1} \qquad \text{with} \quad G_\chi=\mathrm{Gal}(K_\chi/\boldsymbol{Q}).$$

When $g(\chi)$ is prime to p, $e(\phi)$ is an idempotent in the group ring $\boldsymbol{Z}_p[G_\chi]$.

From now on we suppose that K contains ζ_p and that $[K:\boldsymbol{Q}]$ is prime to p. Then $g(\chi)$ is also prime to p and $f(\chi)$ is not divisible by p^2. Further let χ be non-trivial and even. There exists an element $e'(\phi)=\sum_{\sigma\in G_\chi}n_\sigma\sigma^{-1}$ of $\boldsymbol{Z}[G_\chi]$ such that

$$e'(\phi)\equiv e(\phi) \pmod{p\boldsymbol{Z}_p[G_\chi]}, \qquad \sum_{\sigma\in G_\chi}n_\sigma=0.$$

We consider a ϕ-relative cyclotomic unit η_ϕ in the sense of Gras [2] defined by

$$\eta_\phi=(N_\chi(1-\zeta_{f(\chi)}))^{e'(\phi)} \tag{1}$$

with N_χ being the norm from $\boldsymbol{Q}(\zeta_{f(\chi)})$ to K_χ. In the case that $K=\boldsymbol{Q}(\zeta_p)$, it is shown [3] that η_ϕ is a p-th power in K if and only if $(E/E_0E^p)^{e(\phi)}\neq 1$, where E denotes the unit group of K and E_0 the subgroup of E generated by cyclotomic units.

Let ω be a character of $\mathrm{Gal}(K/\boldsymbol{Q})$ of order $p-1$ such that $\omega(\sigma)\equiv a \pmod{p\boldsymbol{Z}_p}$ for each σ in $\mathrm{Gal}(K/\boldsymbol{Q})$, where a is a rational integer satisfying $\zeta_p^\sigma=\zeta_p^a$. We put

$$\bar{\chi}=\chi^{-1}\omega$$

and denote by $\bar{\phi}$ the p-adic character over $\bar{\chi}$. We call $\bar{\phi}$ the reflection of ϕ. Using the first Bernoulli number $B_1(\bar{\chi}^{-1})$ associated with $\bar{\chi}^{-1}$ we introduce a rational integer $m(\bar{\phi})$ such that

$$B_1(\bar{\chi}^{-1})=p^{m(\bar{\phi})}\mu$$

where μ is a unit of $\boldsymbol{Z}_p[\zeta_{g(\bar{\chi})}]$. One has $m(\bar{\phi})\geqq 0$ because $(g(\bar{\chi}), p)=1$ and $\bar{\chi}\neq\omega$. Moreover we define

$$e_K(\bar{\phi})=\frac{1}{[K:\boldsymbol{Q}]}\sum_{\sigma\in \mathrm{Gal}(K/\boldsymbol{Q})}\bar{\phi}(\sigma)\sigma^{-1}.$$

Let A_K be the p-Sylow subgroup of the ideal class group of K. It is known (cf. [2], Theorem I. 2) that

$$p^{m(\bar{\phi})}e_K(\bar{\phi})A_K=0\,.$$

Let $\mathfrak{p}$ be a prime ideal of K lying above p and denote by $N\mathfrak{p}$ its norm. It is clear that $\alpha^{N\mathfrak{p}-1}\equiv 1\ (\mathrm{mod}\, 1-\zeta_p)$ for any integer α in K prime to $1-\zeta_p$. An integer α in K is said to be p-primary if

$$\alpha^{N\mathfrak{p}-1}\equiv 1 \qquad (\mathrm{mod}\,(1-\zeta_p)^p)\,.$$

THEOREM 1. *Let K be an abelian number field containing ζ_p of degree prime to p. Denote by ϕ a non-trivial even p-adic character of the Galois group* $\mathrm{Gal}(K/\boldsymbol{Q})$. *Then a ϕ-relative cyclotomic unit η_ϕ is a p-th power in K if and only if $m(\bar{\phi})>0$ and for any ideal $\mathfrak{a}$, prime to p, representing a class in $e_K(\bar{\phi})A_K$ there is a p-primary integer α in K such that*

$$\mathfrak{a}^{p^{m(\bar{\phi})}}=(\alpha)\,.$$

This result will be proved in Section 5. If a principal ideal $\mathfrak{b}$ of K is not generated by any p-primary integer, then $\mathfrak{b}$ is not a p-th power of a principal ideal of K. Hence we obtain

COROLLARY. *Let the notation and assumptions be as in Theorem* 1. *When $m(\bar{\phi})>0$, it holds that $\eta_\phi\neq\varepsilon^p$ for any unit ε of K if and only if $e_K(\bar{\phi})A_K$ has a cyclic subgroup of order $p^{m(\bar{\phi})}$ generated by an element of A_K containing an ideal, prime to p, whose $p^{m(\bar{\phi})}$-th power is not generated by any p-primary integer.*

§ 3. Cyclotomic units and Jacobi sums.

It is our aim in this section to give a relation between cyclotomic units and certain Jacobi sums. Let χ be an even primitive Dirichlet character modulo $f(\chi)>1$, of order prime to p. We can write either $\chi=\psi$ or $\chi=\psi\omega^k$ with k, $1\leqq k\leqq p-2$, where ψ is a primitive Dirichlet character modulo f, $(f, p)=1$, and ω denotes the Teichmüller character with respect to p, i. e. $\omega(a)\equiv a\ (\mathrm{mod}\, p\boldsymbol{Z}_p)$ for any a in $\boldsymbol{Z}$. For convenience we put $\psi\omega^0=\psi$.

Let $\mathfrak{Q}$ be a prime ideal of $L=\boldsymbol{Q}(\zeta_{fp})$ relatively prime to fp. The residue class ring

$$F_{\mathfrak{Q}}=\boldsymbol{Z}[\zeta_{fp}]/\mathfrak{Q}$$

is a finite field with $N\mathfrak{Q}$ elements, where $N\mathfrak{Q}$ means the norm of $\mathfrak{Q}$. Note that $N\mathfrak{Q}-1$ is divisible by fp. Let $\theta=\theta_{\mathfrak{Q}}$ be a character of the multiplicative cyclic group $F_{\mathfrak{Q}}^*$ of order fp. Put $\theta(0)=0$. We treat the Jacobi sums $J(\theta^a, \theta^b)$

defined by

$$J(\theta^a, \theta^b) = -\sum_{x\in F_{\mathfrak{Q}}} \theta^a(x)\theta^b(1-x)$$

with a, b in $\boldsymbol{Z}$. Let $r=r_{\mathfrak{Q}}$ be a fixed generator of $F_{\mathfrak{Q}}^*$. For each x in $F_{\mathfrak{Q}}^*$ we define a rational integer $\operatorname{ind} x = \operatorname{ind}_{\mathfrak{Q}} x$ by

$$x = r^{\operatorname{ind} x} \quad \text{and} \quad 0 \leqq \operatorname{ind} x \leqq N\mathfrak{Q}-2 .$$

Then one has

$$J(\theta^a, \theta^b) = -\sum_{v=1}^{s} \theta(r)^{av}\theta(r)^{b \operatorname{ind}(1-r^v)} \tag{2}$$

with $s=N\mathfrak{Q}-2$. For a primitive Dirichlet character λ modulo $m>0$ we consider the Gauss sum

$$S(\lambda, \zeta_m) = \sum_{u=0}^{m-1} \lambda(u)\zeta_m^u .$$

It is known that

$$S(\lambda, \zeta_m)S(\lambda^{-1}, \zeta_m) = \lambda(-1)m , \tag{3}$$

$$S(\omega^{-a}, \zeta_p) \equiv (1-\zeta_p)^a/a! \qquad (\operatorname{mod} p\boldsymbol{Z}_p[\zeta_p]) \tag{4}$$

for a, $1\leqq a \leqq p-2$. To describe our results we also need a polynomial $\operatorname{Log}(X)$ in $\boldsymbol{Z}_p[X]$ defined by

$$\operatorname{Log}(1+X) = \sum_{n=1}^{p-1} (-1)^{n+1}X^n/n .$$

Let d be the least common multiple of fp, $p-1$ and $g(\chi)$. All integers in the following are contained in $\boldsymbol{Z}_p[\zeta_d]$.

We now state the following basic lemma.

LEMMA 1. *With the notation as above it holds that*

$$\sum_{c=1}^{p-1} \omega^{-1}(c) \sum_{\sigma\in G_L} \chi\omega^{-1}(\sigma) \operatorname{Log}(J(\theta, \theta^{cf})^\sigma) \equiv 0 \qquad (\operatorname{mod} \mathfrak{P}^p)$$

with $G_L = \operatorname{Gal}(L/\boldsymbol{Q})$ *and* $\mathfrak{P} = (1-\zeta_p)\boldsymbol{Z}_p[\zeta_d]$ *if and only if*

$$\sum_{v=1}^{s} \chi^{-1}(v) \operatorname{ind}(1-r^v) \equiv 0 \qquad (\operatorname{mod} \mathfrak{P}).$$

PROOF. Put $\zeta=\theta(r)$. Then ζ^p (resp. ζ^f) is a primitive f-th (resp. p-th) root of unity. We use the Gauss sums $S(\psi)=S(\psi, \zeta^p)$, $S(\omega^a)=S(\omega^a, \zeta^f)$ with a, $1\leqq a\leqq p-2$. For convenience we set $S(\omega^0)=-1$. We now consider a polynomial $h(X)$ defined by

$$h(X) = -\sum_{v=1}^{s} \zeta^v X^{\operatorname{ind}(1-r^v)}.$$

Since $h(1)=1$ one has

$$\operatorname{Log}(h(1-X)) = \sum_{n=1}^{(p-1)s} \gamma_n X^n$$

with γ_n in $\boldsymbol{Z}_p[\zeta]$. From (2) we obtain

$$\sum_{c=1}^{p-1}\omega^{-1}(c)\sum_{\sigma\in G_L}\chi\omega^{-1}(\sigma)\mathrm{Log}(J(\theta,\theta^{cf})^{\sigma})$$

$$\equiv\sum_{c=1}^{p-1}\omega^{-1}(c)\sum_{\sigma\in G_L}\chi\omega^{-1}(\sigma)\sum_{n=1}^{p-1}\gamma_n^{\sigma}(1-(\zeta^{\sigma})^{cf})^n \qquad (\mathrm{mod}\ \mathfrak{P}^p)$$

$$\equiv S(\omega^{-1})\sum_{\sigma\in G_L}\chi\omega^{-1}(\sigma)\sum_{n=1}^{p-1}\gamma_n^{\sigma}\sum_{i=1}^{n}\binom{n}{i}(-1)^i\omega(i)\omega(\sigma) \qquad (\mathrm{mod}\ \mathfrak{P}^p)$$

$$\equiv -S(\omega^{-1})\sum_{\sigma\in G_L}\chi(\sigma)\gamma_1^{\sigma} \qquad (\mathrm{mod}\ \mathfrak{P}^p)$$

because $\binom{n}{i}\omega(i)\equiv n\binom{n-1}{i-1}$ (mod $\mathfrak{P}^{p-1}$) holds if $1\leqq i\leqq n\leqq p-1$. It is easy to see

$$\gamma_1=\sum_{v=1}^{s}\zeta^v\mathrm{ind}(1-r^v).$$

Hence we compute

$$\sum_{\sigma\in G_L}\chi(\sigma)\gamma_1^{\sigma}=\sum_{i=1}^{p-1}\sum_{\substack{j=1\\(j,f)=1}}^{f-1}\chi(if+jp)\sum_{v=1}^{s}\zeta^{(if+jp)v}\mathrm{ind}(1-r^v)$$

$$\equiv\psi(p)\omega^k(f)S(\psi)S(\omega^k)\sum_{v=1}^{s}\chi^{-1}(v)\mathrm{ind}(1-r^v) \qquad (\mathrm{mod}\ \mathfrak{P}^{p-1}).$$

It follows from (3) and (4) that $S(\psi)S(\omega^k)$ is not divisible by $\mathfrak{P}^{p-1}$. Since $g(\chi)$ is prime to p, we have

$$\mathfrak{P}\cap\boldsymbol{Z}_p[\zeta_{g(\chi)}]=p\boldsymbol{Z}_p[\zeta_{g(\chi)}].$$

Thus any integer α in $\boldsymbol{Q}_p(\chi)$ satisfying $\alpha\equiv 0$ (mod $\mathfrak{P}$) is divisible by $\mathfrak{P}^{p-1}$. This proves the lemma.

In the rest of this section we shall show the following

THEOREM 2. *Let χ be an even primitive Dirichlet character modulo $f(\chi)>1$, of order prime to p, and let ϕ be the p-adic character over χ. Denote by fp the least common multiple of p and $f(\chi)$ with f prime to p. Then a ϕ-relative cyclotomic unit η_ϕ is a p-th power in $L=\boldsymbol{Q}(\zeta_{fp})$ if and only if*

$$\sum_{c=1}^{p-1}\omega^{-1}(c)\sum_{\sigma\in G_L}\phi\omega^{-1}(\sigma)\mathrm{Log}(J(\theta_{\mathfrak{Q}},\theta_{\mathfrak{Q}}^{cf})^{\sigma})\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{P}^p) \tag{5}$$

holds for any prime ideal $\mathfrak{Q}$ of L prime to fp, and for any character $\theta_{\mathfrak{Q}}$ of $F_{\mathfrak{Q}}^*$ of order fp, where $G_L=\mathrm{Gal}(L/\boldsymbol{Q})$ and $\mathfrak{P}=(1-\zeta_p)\boldsymbol{Z}_p[\zeta_d]$.

LEMMA 2. *Let the notation and assumptions be as in Theorem 2. Then η_ϕ is a p-th power in L if and only if for any prime ideal $\mathfrak{Q}$ of L not dividing fp, and for any τ in $H=\mathrm{Gal}(\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p)$*

$$\sum_{v=1}^{s}\chi^{-1}(v)^{\tau}\mathrm{ind}_{\mathfrak{Q}}(1-r^v)\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{P}) \tag{6}$$

is valid with $s=N\mathfrak{Q}-2$.

PROOF. Let $\mathfrak{Q}$ be a prime ideal of L with $(\mathfrak{Q}, fp)=1$. First we note that the left hand side of (6) is equal to

$$\sum_{v=1}^{f(\chi)-1} \chi^{-1}(v)^{\tau} \sum_{w=0}^{t-1} \mathrm{ind}_{\mathfrak{Q}}(1-r^{v+wf(\chi)})$$

with $t=(N\mathfrak{Q}-1)/f(\chi)$. Choose an integer β in L representing a generator $r_{\mathfrak{Q}}$ of the cyclic group $F_{\mathfrak{Q}}^{*}$. One has

$$\prod_{w=0}^{t-1}(1-\beta^{v+wf(\chi)})\equiv 1-\beta^{tv} \qquad (\mathrm{mod}\, \mathfrak{Q}).$$

Remark that $\beta^{t}\equiv\xi$ (mod $\mathfrak{Q}$) for a certain primitive $f(\chi)$-th root ξ of unity. We may put $\zeta_{f(\chi)}=\xi$ in the definition (1). Let y be the residue class in $F_{\mathfrak{Q}}$ represented by η_{ϕ}. For any σ in G_L we can see

$$(7) \qquad \mathrm{ind}_{\mathfrak{Q}}\, y^{\sigma}\equiv g(\chi)^{-1}\sum_{\tau\in H}\chi(\sigma)^{\tau}\sum_{v=1}^{s}\chi^{-1}(v)^{\tau}\mathrm{ind}_{\mathfrak{Q}}(1-r_{\mathfrak{Q}}^{v}) \qquad (\mathrm{mod}\, \mathfrak{P}).$$

Take an automorphism ρ in G_L whose restriction to K_{χ} generates the cyclic group G_{χ}. Then

$$\sum_{l=0}^{g(\chi)-1} \chi^{-1}(\rho^{l})^{\tau}\mathrm{ind}_{\mathfrak{Q}}(y^{\rho^{l}})$$

is congruent to the left hand side of (6) modulo $\mathfrak{P}$. Thus if η_{ϕ} is a p-th power in L then $\mathrm{ind}_{\mathfrak{Q}}\, y^{\sigma}\equiv 0$ (mod p) for any $\mathfrak{Q}$ and for any σ in G_L, and hence the congruence (6) is true for any $\mathfrak{Q}$ and for any τ.

Conversely we assume that $\eta_{\phi}\neq\varepsilon^{p}$ for any unit ε of L. Since L contains ζ_p, the field $L(\eta_{\phi}^{1/p})$ is a normal extension of L of degree p. It is known that there are infinitely many prime ideals of L, relatively prime to fp, which remain prime in $L(\eta_{\phi}^{1/p})$. For such a prime ideal $\mathfrak{Q}$ it is shown that $\mathrm{ind}_{\mathfrak{Q}}\, y\not\equiv 0$ (mod p). Indeed, if $\eta_{\phi}\equiv\alpha^{p}$ (mod $\mathfrak{Q}$) with some integer α in L, then $\eta_{\phi}^{1/p}\zeta_{p}^{u}\equiv\alpha$ (mod $\mathfrak{Q}$) for any u in $\boldsymbol{Z}$. This gives a contradiction because $(\mathfrak{Q}, 1-\zeta_p)=1$. Hence from (7) we see that (6) does not hold for this prime ideal. Thus the proof is complete.

PROOF OF THEOREM 2. For any τ in H, χ^{τ} is also a character under ϕ. We set

$$C(\chi^{\tau}, \theta_{\mathfrak{Q}})=\sum_{c=1}^{p-1}\omega^{-1}(c)\sum_{\sigma\in G_L}\chi^{\tau}\omega^{-1}(\sigma)\mathrm{Log}(J(\theta_{\mathfrak{Q}}, \theta_{\mathfrak{Q}}^{cf})^{\sigma}).$$

Then $\sum_{\tau\in H}C(\chi^{\tau}, \theta_{\mathfrak{Q}})$ is equal to the left hand side of (5). Further let ρ be as in the proof of Lemma 2. We have

$$J(\theta_{\mathfrak{Q}}, \theta_{\mathfrak{Q}}^{cf})^{\rho}=J(\theta_{\mathfrak{Q}}^{b}, \theta_{\mathfrak{Q}}^{bcf})$$

for some integer b in $\boldsymbol{Z}$, prime to fp. Hence it follows that

$$\sum_{l=0}^{g(\chi)-1}\chi\omega^{-1}(b^{l})^{\tau'}\sum_{\tau\in H}C(\chi^{\tau}, \theta_{\mathfrak{Q}}^{b^{l}})$$

$$=\sum_{l=0}^{g(\chi)-1}\chi\omega^{-1}(b^l)^{\tau'}\sum_{\tau\in H}\chi^{-1}\omega(b^l)^{\tau}C(\chi^{\tau},\ \theta_{\mathfrak{Q}})$$

$$=g(\chi)C(\chi^{\tau'},\ \theta_{\mathfrak{Q}})$$

for any τ' in H. Note that the order of $\theta_{\mathfrak{Q}}^{b^l}$ is also equal to fp. Applying Lemmas 1, 2 we obtain the assertion of Theorem 2.

§4. Prime factorization of Jacobi sums.

In this section let χ be an odd primitive Dirichlet character modulo $f(\chi)$ such that $(g(\chi),\ p)=1$ and $\chi\neq\omega$. We denote by ϕ the p-adic character over χ. We recall the first Bernoulli number $B_1(\chi^{-1})$ associated with χ^{-1} defined as follows:

$$B_1(\chi^{-1})=f(\chi)^{-1}\sum_{u=0}^{f(\chi)-1}\chi^{-1}(u)u\ .$$

As in Section 2 we consider an invariant $m(\phi)$ such that $B_1(\chi^{-1})=p^{m(\phi)}\mu$ with a unit μ in $\boldsymbol{Z}_p[\zeta_{g(\chi)}]$. It is clear that $m(\phi)$ is determined independently of the choice of a character χ under ϕ.

Let fp be the least common multiple of p and $f(\chi)$ with f prime to p. Take a prime ideal $\mathfrak{Q}$ of $L=\boldsymbol{Q}(\zeta_{fp})$ not dividing fp. Moreover let θ be a character of $F_{\mathfrak{Q}}^{*}$ of order fp such that if a residue class $x\neq 0$ in $F_{\mathfrak{Q}}$ contains an integer α satisfying $\alpha^{(N\mathfrak{Q}-1)/fp}\equiv\zeta_{fp}\ (\mathrm{mod}\,\mathfrak{Q})$, then $\theta(x)=\zeta_{fp}$. It is known (for instance, cf. [4]) that for rational integers a, b with $a+b\not\equiv 0\ (\mathrm{mod}\, fp)$,

$$\mathfrak{Q}^{d(a,b)}=(J(\theta^{a},\ \theta^{b})) \tag{8}$$

where

$$d(a,\ b)=\sum_{\substack{0<u<fp\\(u,fp)=1}}\left(\left\langle\frac{au}{fp}\right\rangle+\left\langle\frac{bu}{fp}\right\rangle-\left\langle\frac{(a+b)u}{fp}\right\rangle\right)\sigma_u^{-1}.$$

Here for a real number s we mean by $\langle s\rangle$ its fractional part; namely $0\leqq\langle s\rangle<1$ and $s-\langle s\rangle$ is in $\boldsymbol{Z}$. Further σ_u denotes the automorphism of L such that $\zeta_{fp}^{\sigma_u}=\zeta_{fp}^{u}$. If $a\not\equiv 0\ (\mathrm{mod}\,fp)$ then $J(\theta^{a},\ \theta^{-a})=1$. So we may put $d(a,\ -a)=0$ in this case.

For each automorphism σ of L let σ' be its restriction to K_{χ}. By simple calculation we can see that

$$\sum_{u}\left\langle\frac{cu}{fp}\right\rangle(\sigma_u')^{-1}e(\phi)=g(\chi)^{-1}\sum_{\tau\in H}\sum_{u}\chi^{-1}(u)^{\tau}\left\langle\frac{cu}{fp}\right\rangle\sum_{\sigma\in G_{\chi}}\chi(\sigma)^{\tau}\sigma^{-1} \tag{9}$$

for any c in $\boldsymbol{Z}$, where u runs over the integers such that $0<u<fp$, $(u,\ fp)=1$, and $H=\mathrm{Gal}(\boldsymbol{Q}_p(\chi)/\boldsymbol{Q}_p)$. Also we compute

$$\sum_{u}\chi^{-1}(u)\left\langle\frac{cu}{fp}\right\rangle=t_{\chi}(c)B_1(\chi^{-1})$$

where

$$(10)\qquad t_\chi(c)=\begin{cases}(p-1)\chi(c/p) & \text{if } f(\chi)=f \text{ and } p\mid c,\\ (1-\chi^{-1}(p))\chi(c) & \text{otherwise.}\end{cases}$$

For a, b in $\boldsymbol{Z}$ let $d'(a, b)$ be the element of $\boldsymbol{Z}[G_\chi]$ induced from $d(a, b)$ by restriction. A theorem of Leopoldt [6] shows that $d'(a, b)$ annihilates the ideal class group of K_χ. From (9) we get

$$(11)\qquad d'(a, b)e(\phi)=p^{m(\phi)}g(\chi)^{-1}\sum_{\tau\in H}\mu(a, b)^\tau\sum_{\sigma\in G_\chi}\chi(\sigma)^\tau\sigma^{-1}$$

$$\text{with}\quad \mu(a, b)=(t_\chi(a)+t_\chi(b)-t_\chi(a+b))B_1(\chi^{-1})/p^{m(\phi)}.$$

Note that $\mu(a, b)$ is contained in $\boldsymbol{Z}_p[\zeta_{g(\chi)}]$. By (10) we have

$$\sum_{c=1}^{p-1}\omega^{-1}(c)\mu(1, cf)\equiv\sum_{c=1}^{p-1}\omega^{-1}(c)t_\chi(1+cf)\not\equiv 0 \pmod{p\boldsymbol{Z}_p[\zeta_{g(\chi)}]}$$

because $\chi(1+cf)=\omega^l(1+cf)\equiv(1+cf)^l \pmod{p\boldsymbol{Z}_p}$ for some l in $\boldsymbol{Z}$. We now put

$$\delta=\sum_{c=1}^{p-1}\omega^{-1}(c)d'(1, cf)\,.$$

It follows from (11) that

$$\delta e(\phi)=p^{m(\phi)}g(\chi)^{-1}\sum_{\tau\in H}\mu^\tau\sum_{\sigma\in G_\chi}\chi(\sigma)^\tau\sigma^{-1}$$

with a unit μ in $\boldsymbol{Z}_p[\zeta_{g(\chi)}]$. Let $\Phi(X)$ be a polynomial in $\boldsymbol{Z}_p[X]$ such that $\Phi(\chi(\rho))=\mu^{-1}$, where ρ is a generator of the cyclic group G_χ. Putting $\gamma=\Phi(\rho)$ we obtain

$$(12)\qquad \gamma\delta e(\phi)=p^{m(\phi)}e(\phi)\,.$$

The above argument implies that

$$(13)\qquad p^{m(\phi)}e(\phi)A_{K_\chi}=0\,.$$

§ 5. Proof of Theorem 1.

In this section let the notation and assumptions be as in Theorem 1. Denote by χ a character of $\mathrm{Gal}(K/\boldsymbol{Q})$ under ϕ. We regard χ as a Dirichlet character and write $\chi=\phi\omega^k$ with k, $0\leqq k\leqq p-2$, where ϕ is a primitive Dirichlet character modulo f, $(f, p)=1$, and ω denotes the Teichmüller character with respect to p. Then $\tilde{\chi}=\phi^{-1}\omega^{1-k}$. We put $L=\boldsymbol{Q}(\zeta_{fp})$.

We start with the following

LEMMA 3. *Let K', M be number fields contained in L such that $K'\subset M$ and $[M:K']=p$. If the degree $[K':\boldsymbol{Q}]$ is not divisible by p, then there exists a prime ideal of K', relatively prime to p, which is ramified in M.*

PROOF. Since M is an abelian extension of $\boldsymbol{Q}$ and $g'=[K':\boldsymbol{Q}]$ is prime to p, there exists an extension M' of $\boldsymbol{Q}$ of degree p such that $M'K'=M$. We can find a prime q ramified in M'. Because $(g', p)=1$, any prime ideal of K' lying above q is ramified in M. On the other hand the ramification index of $\mathfrak{p}_0$ over p is $p-1$, where $\mathfrak{p}_0$ means a prime ideal of L lying above p. Thus $q\neq p$. This proves the lemma.

We recall some properties of the polynomial $\mathrm{Log}(X)$. Put $\pi=1-\zeta_p$. One knows (for instance, cf. [1]) that for any integers α, β in $\bar{\boldsymbol{Q}}_p$ satisfying $\alpha\equiv\beta\equiv 1 \pmod{\pi}$,

$$\text{(14)} \qquad \mathrm{Log}(\alpha\beta)\equiv\mathrm{Log}(\alpha)+\mathrm{Log}(\beta) \pmod{\pi^p}.$$

Denote by $N\mathfrak{p}$ the norm of a prime ideal $\mathfrak{p}$ of K lying above p. Since $(N\mathfrak{p}-1, p)=1$, it is seen that an integer α in K is p-primary if and only if $\mathrm{Log}(\alpha)\equiv 0 \pmod{\pi^p}$. In particular if $\alpha=\beta^p$ with β in K then α is p-primary. We define a polynomial $\mathrm{Exp}(X)$ in $\boldsymbol{Z}_p[X]$ by

$$\mathrm{Exp}(X)=\sum_{n=0}^{p-1} X^n/n!\,.$$

Then $\mathrm{Log}(\mathrm{Exp}(\alpha))\equiv\alpha \pmod{\pi^p}$ for any integer α in $\bar{\boldsymbol{Q}}_p$ divisible by π.

Let $\varepsilon=\eta_\phi^{1/p}$ be a p-th root of η_ϕ. Assume that ε is not contained in $K'=K_\chi(\zeta_p)$. Then $K'(\varepsilon)$ is an extension of K' of degree p. Note that $K'\subset K\cap L$. Since $[K:K']$ is prime to p, K does not contain ε. If ε is in L, by Lemma 3 we can find a prime ideal $\mathfrak{q}$ of K', prime to p, which is ramified in $K'(\varepsilon)$. On the other hand $\mathfrak{q}$ does not divide the discriminant

$$\prod_{0\leq i,j\leq p-1}(\varepsilon\zeta_p^i-\varepsilon\zeta_p^j)=\pm\eta_\phi^{p-1}p^p.$$

Hence ε is not a unit of L. This implies that ε is contained in K if and only if it is in L.

Next we remark that $\sigma e_K(\bar{\phi})=e_K(\bar{\phi})$ for any σ in $\mathrm{Gal}(K/K_{\bar{\chi}})$. Let $\mathfrak{a}_0$ be an ideal of K representing a class c in $e_K(\bar{\phi})A_K$. Then $\mathfrak{a}=N_{\bar{\chi}}\mathfrak{a}_0$ represents $\bar{g}c$, where $N_{\bar{\chi}}$ means the norm from K to $K_{\bar{\chi}}$ and $\bar{g}=[K:K_{\bar{\chi}}]$. Since $(\bar{g}, p)=1$, the class c is also represented by $\mathfrak{a}^t$ for some $t>0$. Hence

$$\mathfrak{a}_0(\alpha_1)=\mathfrak{a}^t(\alpha_2)$$

with α_1, α_2 being integers in K. If the p^l-th power of $\mathfrak{a}$ is a principal ideal generated by a p-primary integer in $K_{\bar{\chi}}$ for $l>0$, then $\mathfrak{a}_0^{p^l}=(\alpha)$ holds with α p-primary. Conversely we take an ideal $\mathfrak{b}$ of $K_{\bar{\chi}}$ contained in a class in $e(\bar{\phi})A_{K_{\bar{\chi}}}$. Let $\mathfrak{b}_0$ be the ideal of K induced from $\mathfrak{b}$. It is easy to see that $\mathfrak{b}_0$ represents a class in $e_K(\bar{\phi})A_K$. Suppose that $\mathfrak{b}_0^{p^l}=(\beta)$ holds with β in K and $l>0$. We have $\mathfrak{b}^{\bar{g}p^l}=(N_{\bar{\chi}}\beta)$. If β were p-primary, the p^l-th power of $\mathfrak{b}$ would be originally generated by a p-primary integer in $K_{\bar{\chi}}$. Applying the above arguments we rewrite the assertion of Theorem 1 as follows: η_ϕ is a p-th power in L if and only if $m(\bar{\phi})>0$ and for any ideal $\mathfrak{a}$, prime to p, representing a class in $e(\bar{\phi})A_{K_{\bar{\chi}}}$, the $p^{m(\bar{\phi})}$-th power of $\mathfrak{a}$ is generated by a p-primary integer in $K_{\bar{\chi}}$.

For simplicity of notation, from now on we put $K=K_{\bar{\chi}}$ and use g, G instead of $g(\bar{\chi})$, $G_{\bar{\chi}}$ respectively.

Let E be the unit group of K. Since $\bar{\phi}$ is odd and is different from ω, one has

$$(E/E^{p})^{e(\bar{\phi})}=1\,. \tag{15}$$

By n we mean a sufficiently large natural number. For each p-adic integer α we define a positive rational integer $[\alpha]$ by the congruence

$$[\alpha]\equiv\alpha \qquad (\mathrm{mod}\ p^{n}\boldsymbol{Z}_{p}).$$

Let $p^{n'}h$ be the class number of K where $n'\geqq 0$ and $(h, p)=1$. We put

$$e'(\bar{\phi})=\sum_{\sigma\in G}[g^{-1}\bar{\phi}(\sigma)]\sigma^{-1}.$$

Then we derive from (13) that

$$\mathfrak{a}^{p^{m(\bar{\phi})}he'(\bar{\phi})} \quad \text{is principal} \tag{16}$$

for any ideal $\mathfrak{a}$ of K. Next for c, $1\leqq c\leqq p-1$, we consider the element $d'(1, cf)$ of $\boldsymbol{Z}[G]$ induced from $d(1, cf)$, which is defined as in (8), by restriction. We set

$$\delta'=\sum_{c=1}^{p-1}c'd'(1, cf)$$

with $c'=[\omega^{-1}(c)]$. Applying (8) one sees that for any prime ideal $\mathfrak{Q}$ of L relatively prime to fp,

$$(N_{L/K}\mathfrak{Q})^{\delta' e'(\bar{\phi})}=(\alpha(\theta_{\mathfrak{Q}})) \tag{17}$$

$$\text{with}\quad \alpha(\theta_{\mathfrak{Q}})=\prod_{c=1}^{p-1}(N_{L/K}J(\theta_{\mathfrak{Q}}, \theta_{\mathfrak{Q}}^{cf}))^{c'e'(\bar{\phi})},$$

where $\theta_{\mathfrak{Q}}$ is a suitable character of $F_{\mathfrak{Q}}^{*}$ of order fp and $N_{L/K}$ denotes the norm from L to K.

We are now ready to prove the theorem. Let d be the least common multiple of fp, $p-1$ and g. As in Section 3 we put $\mathfrak{P}=(1-\zeta_{p})\boldsymbol{Z}_{p}[\zeta_{d}]$. First we suppose that η_{ϕ} is a p-th power in L. It follows from (14) and Theorem 2 that

$$\begin{aligned}\mathrm{Log}(\alpha(\theta_{\mathfrak{Q}}))&\equiv g^{-1}\sum_{c=1}^{p-1}\omega^{-1}(c)\sum_{\sigma\in G_{L}}\bar{\phi}(\sigma^{-1})\mathrm{Log}(J(\theta_{\mathfrak{Q}}, \theta_{\mathfrak{Q}}^{cf})^{\sigma}) &&(\mathrm{mod}\ \mathfrak{P}^{p})\\ &\equiv 0 &&(\mathrm{mod}\ \mathfrak{P}^{p})\end{aligned} \tag{18}$$

for any prime ideal $\mathfrak{Q}$ of L not dividing fp, where $G_{L}=\mathrm{Gal}(L/\boldsymbol{Q})$. So $\alpha(\theta_{\mathfrak{Q}})$ is

p-primary. By (12) we have

$$\gamma'\delta' e'(\bar{\phi}) \equiv p^{m(\bar{\phi})} e'(\bar{\phi}) \qquad (\mathrm{mod}\ p^n \boldsymbol{Z}[G])$$

for some element γ' of $\boldsymbol{Z}[G]$. Hence for any $\mathfrak{Q}$ we can find a p-primary integer α in K such that

$$(19) \qquad (N_{L/K}\mathfrak{Q})^{p^{m(\bar{\phi})} h e'(\bar{\phi})} = (\alpha).$$

Although the claim that $m(\bar{\phi})>0$ can be derived from a congruence of Gras (cf. [2], [7]), we shall show it in another way. For this purpose we define an integer β' in L by

$$\beta' = \begin{cases} \sum_{\sigma \in G} [\bar{\phi}(\sigma^{-1})](\zeta_f \zeta_p)^{\bar{\sigma}} & \text{if} \quad k \neq 1, \\ p \sum_{\sigma \in G} [\bar{\phi}(\sigma^{-1})]\zeta_f^{\bar{\sigma}} & \text{if} \quad k=1, \end{cases}$$

where for each σ in G, $\bar{\sigma}$ means an automorphism in G_L whose restriction to K coincides with σ. It is clear that $\beta' \equiv 0 \ (\mathrm{mod}\ \mathfrak{P})$. Choose an integer β in L such that $\beta \equiv \mathrm{Exp}(\beta') \ (\mathrm{mod}\ \mathfrak{P}^p)$ and (β) is prime to fp. Assume that $m(\bar{\phi})=0$. Because $e'(\bar{\phi})^2 \equiv e'(\bar{\phi}) \ (\mathrm{mod}\ p^n \boldsymbol{Z}[G])$, it is shown from (15) and (19) that

$$\mathrm{Log}((N_{L/K}(\beta))^{e'(\bar{\phi})}) \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{P}^p).$$

On the other hand, we put

$$S'(\psi) = \sum_{u=0}^{p-1} [\sum_{\tau \in H} \psi(u)^\tau] \zeta_f^u, \qquad S'(\omega^{k-1}) = \sum_{v=0}^{p-1} [\omega^{k-1}(v)] \zeta_p^v$$

for $k \neq 1$, and $S'(\omega^0) = -p$, where $H = \mathrm{Gal}(\boldsymbol{Q}_p(\bar{\chi})/\boldsymbol{Q}_p)$. It is easy to see that

$$\sum_{\rho \in G} [g^{-1}\bar{\phi}(\rho)][\bar{\phi}(\sigma^{-1}\rho^{-1})] \equiv [\bar{\phi}(\sigma^{-1})] \equiv [\sum_{\tau \in H} \psi(\sigma)^\tau][\omega^{k-1}(\sigma)] \qquad (\mathrm{mod}\ p^n)$$

is valid for any σ in G. Hence we get

$$\begin{aligned} \mathrm{Log}((N_{L/K}(\beta))^{e'(\bar{\phi})}) &\equiv e'(\bar{\phi}) \sum_{\sigma \in \mathrm{Gal}(L/K)} (\beta')^\sigma \qquad (\mathrm{mod}\ \mathfrak{P}^p) \\ &\equiv S'(\psi) S'(\omega^{k-1}) \qquad (\mathrm{mod}\ \mathfrak{P}^p). \end{aligned}$$

Since $S'(\omega^{k-1})$ is not divisible by $\mathfrak{P}^p$, we have

$$\sum_{\tau \in H} S(\psi^\tau, \zeta_f) \equiv S'(\psi) \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{P}).$$

Changing ζ_f by any conjugate of ζ_f in the above argument, we can gain the same conclusion. Let b be a rational integer such that $\psi(b)$ is a primitive $g(\psi)$-th root of unity. Then we see

$$S(\psi, \zeta_f) = g(\psi)^{-1} \sum_{i=1}^{g(\psi)} \psi(b^i) \sum_{\tau \in H} S(\psi^\tau, \zeta_f^{b^i}) \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{P}).$$

This is contradictory to (3). Thus we have shown $m(\bar{\phi})>0$.

Let I be the group of fractional ideals of K and I_0 the subgroup of all principal ideals in I. Assume that there is a class in $e(\bar{\phi})A_K$ containing an ideal $\mathfrak{a}$ prime to p such that

$$\mathfrak{a}^{p^{m(\bar{\phi})}} \neq (\alpha) \tag{20}$$

for any p-primary integer α in K. Let $H_1 = I^p I_0$. Remark that $\mathfrak{a}$ is not contained in H_1. By M_1 we denote the class field belonging to H_1. Then M_1 is the maximal unramified elementary abelian p-extension of K. From Lemma 3 we have $M_1 \cap L = K$. Hence by class field theory one can find a prime ideal $\mathfrak{q}$ of K, totally decomposed in L, such that $(\mathfrak{q}, fp) = 1$ and $\mathfrak{a}H_1 = \mathfrak{q}H_1$. Thus $\mathfrak{q} = N_{L/K}\mathfrak{Q}$ for some prime ideal $\mathfrak{Q}$ of L not dividing fp, and

$$\mathfrak{a}\mathfrak{c}_1 = \mathfrak{q}\mathfrak{c}_2$$

for some ideals $\mathfrak{c}_1$, $\mathfrak{c}_2$ in H_1. As $\mathfrak{a}$ represents a class in $e(\bar{\phi})A_K$ and $(h, p) = 1$, there exist integers β_1, β_2 in K and t in $\boldsymbol{Z}$ such that

$$\mathfrak{a}(\beta_1) = \mathfrak{a}^{hte'(\bar{\phi})}(\beta_2)\,.$$

We may assume that $\mathfrak{c}_1$, $\mathfrak{c}_2$, (β_1) and (β_2) are all prime to p. Observing $m(\bar{\phi}) > 0$, we obtain by (16) that the $p^{m(\bar{\phi})}he'(\bar{\phi})$-th power of $\mathfrak{c}_i$ is a p-th power of a principal ideal for $i = 1, 2$. Hence it follows from (19) that $\mathfrak{a}^{p^{m(\bar{\phi})}} = (\alpha)$ with α p-primary. This is contrary to (20). Thus we have proved a half of the assertion.

Next we suppose that $\eta_\phi \neq \varepsilon^p$ for any unit ε of L and that $m(\bar{\phi}) > 0$. By means of Theorem 2 we can find a prime ideal $\mathfrak{Q}$ of L, prime to fp, for which (18) is not valid. If we put $\mathfrak{b} = (N_{L/K}\mathfrak{Q})^{\delta' e'(\bar{\phi})/p^{m(\bar{\phi})}}$ then $\mathfrak{b}$ represents a class in $e(\bar{\phi})A_K$ and

$$\mathfrak{b}^{p^{m(\bar{\phi})}} = (\beta) \qquad \text{with} \quad \beta = \alpha(\theta_{\mathfrak{Q}}).$$

Here β is not p-primary. Any integer α in K which generates the $p^{m(\bar{\phi})}$-th power of $\mathfrak{b}$ is written as $\alpha = \eta\beta$ with a unit η of K. Applying (15) and (17) we compute

$$\begin{aligned} e'(\bar{\phi})\operatorname{Log}(\alpha) &\equiv \operatorname{Log}(\eta^{e'(\bar{\phi})}) + \operatorname{Log}(\beta^{e'(\bar{\phi})}) && (\operatorname{mod} \mathfrak{P}^p) \\ &\equiv \operatorname{Log}(\beta) \not\equiv 0 && (\operatorname{mod} \mathfrak{P}^p). \end{aligned}$$

This implies $\operatorname{Log}(\alpha) \not\equiv 0 \ (\operatorname{mod} \mathfrak{P}^p)$. Therefore the $p^{m(\bar{\phi})}$-th power of $\mathfrak{b}$ is not generated by any p-primary integer in K. This completes the proof.

References

[1] Z. I. Borevich and I. R. Shafarevich, Number theory, Academic Press, London and New York, 1966.

[2] G. Gras, Classes d'idéaux des corps abeliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier (Grenoble), **27** (1977), 1-66.
[3] K. Iwasawa, A note on cyclotomic fields, Invent. Math., **36** (1976), 115-123.
[4] S. Lang, Cyclotomic fields, Springer-Verlag, New York, 1978.
[5] H. W. Leopoldt, Zur Struktur der l-Klassengruppe galoisscher Zahlkörper, J. Reine Angew. Math., **199** (1958), 165-174.
[6] H. W. Leopoldt, Zur Arithmetik in abelschen Zahlkörpern, J. Reine Angew. Math., **209** (1962), 54-71.
[7] T. Uehara, On some congruences for generalized Bernoulli numbers, Rep. Fac. Sci. Engrg. Saga Univ. Math., **10** (1982), 1-8.
[8] A. Wiles, Modular curves and the class group of $Q(\zeta_p)$, Invent. Math., **58** (1980), 1-35.

Tsuyoshi UEHARA
Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840
Japan