Tohoku Math. J.
57 (2005), 541–557

THAINE'S ANNIHILATOR

KOICHI TATEYAMA

(Received December 1, 2003, revised September 24, 2004)

Abstract. The aim of this paper is to give, for any real cyclotomic field, elements of the group ring of the Galois group which annihilate the ideal class group. Our annihilators are constructed by using the prime decomposition of an element which is an analogy of the Gaussian sum. This method is essentially due to Thaine.

1. Introduction. For a positive integer N, we put $\zeta_N = \exp(2\pi\sqrt{-1}/N)$. In this paper, we fix a positive integer m and a cyclotomic field $k = \boldsymbol{Q}(\zeta_m)$. We assume that m is the conductor of k. Let E be the group of units of k and let $G = \mathrm{Gal}(k/\boldsymbol{Q})$. Let $\Delta = \Delta_m$ be the subgroup of $k^\times$ generated by $\{1-\zeta_m^a \mid 0 < a < m,\ a \in \boldsymbol{Z}\}$. We let $D = \Delta \cdot E \subset k^\times$. For any $u \in \mathrm{Hom}(D, \boldsymbol{Z})$ and an integer t which is not divisible by m, we set $\varepsilon(t) = \zeta_m^t - 1$ and define $\theta(u, \varepsilon(t)) \in \boldsymbol{Z}[G]$ by

$$\theta(u, \varepsilon(t)) = \sum_{\sigma\in G} u(\varepsilon(t)^\sigma)\sigma^{-1} .$$

By a simple computation, we can show that $\theta(u, \varepsilon(t))$ is an element of $(1 + j)\boldsymbol{Z}[G]$, where j is the complex conjugation in G. Moreover, we can prove the following theorem.

THEOREM 1.1. *$2\theta(u, \varepsilon(t))$ annihilates the ideal class group of $\boldsymbol{Q}(\zeta_m)$.*

$\theta(u, \varepsilon(t))$ is constructed by using some cyclotomic units. This remarkable method was initiated by Thaine ([T]). It was proved in [T] that for an ideal class c, there is an annihilator θ_c of c. Moreover, we prove that $2\theta_c$ annihilates all elements of the ideal class group (see Proposition 3.2 and Theorem 3.7). Hence, the assumption that the order of an ideal class is prime to $[\boldsymbol{Q}(\zeta_m) : \boldsymbol{Q}]$ is not neccesary for our proof of Theorem 1.1 (see [T], §4).

Let $f > 1$ be a divisor of m and χ a Dirichlet character of conductor f. We set

$$u(\chi) = \sum_{a=1}^{f-1} u(\zeta_f^a - 1)\chi(a) .$$

Let $\{\varepsilon_i\}$ be a system of fundamental units in $k^+ = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ and let $G^+ = \mathrm{Gal}(k^+/\boldsymbol{Q})$. We define

$$R_u = \det_{\sigma,i}(u(\varepsilon_i^\sigma)) ,$$

where $\sigma \in G^+ - \{1\}$ and $0 < i < [k^+ : \mathrm{Q}]$. In Section 4, we prove the following class number formula.

2000 *Mathematics Subject Classification.* Primary 11R29.

THEOREM 1.2. *If $R_u \neq 0$, then*

$$h^+ R_u = \pm \prod_{\chi(-1)=1,\, \chi\neq 1} \frac{1}{2} u(\chi)\,,$$

where h^+ is the class number of k^+ and the product is taken over the nontrivial Dirichlet characters χ that are even.

Essentially, this formula is deduced from the classical class number formula. However, we note that all factors of the formula are algebraic integers.

In Section 5, we study the index $[R^+ : S(\varDelta)]$, where $R^+ = (1+j)\boldsymbol{Z}[G]$ and $S(\varDelta)$ is the G-submodule of R^+ generated by $\{\theta_u(\eta) \mid u \in \mathrm{Hom}(D, \boldsymbol{Z}), \eta \in \varDelta\}$.

2. 1-cocycle of a unit group. We denote by O_F the ring of integers of a number field F and by E_F the group of units of O_F. Let k be a finite extension of $\boldsymbol{Q}$, and K a finite Galois extension field over k. Let $\varGamma = \mathrm{Gal}(K/k)$ and let $z = \{z_\sigma \mid \sigma \in \varGamma\}$ be a 1-cocycle with values in E_K. The linear independence of automorphisms in $\varGamma$ implies that there exists $\lambda \in K^\times$ with

$$g(z, \lambda) = \sum_{\sigma\in\varGamma} z_\sigma \lambda^\sigma \neq 0\,.$$

Since $g(z,\lambda)^\tau = z_\tau^{-1} g(z,\lambda)$ for $\tau \in \varGamma$, we have the following decomposition of ideals:

$$(g(z,\lambda)) = \mathfrak{A}(k) \prod_{i=1}^{r} \mathfrak{P}_i^{s_i}\,,$$

where $\mathfrak{A}(k)$ is the lift of an ideal of k , $\mathfrak{P}_i$ $(1 \leq i \leq r)$ is a prime of K which is ramified over k and s_i is the exponent of $\mathfrak{P}_i$ in the decomposition of $(g(z,\lambda))$. Let T be the inertia group of $\mathfrak{P} = \mathfrak{P}_1$ over k. Since $z_{\sigma\tau} \equiv z_\sigma z_\tau \bmod \mathfrak{P}$ for $\sigma, \tau \in T$, the map $\sigma \mapsto z_\sigma \bmod \mathfrak{P}$ is an element of $\mathrm{Hom}(T,\ (O_K/\mathfrak{P})^\times)$. Let p be the characteristic of $O_K/\mathfrak{P}$ and $e = e_0 p^r$ $((e_0, p) = 1)$ the ramification index of $\mathfrak{P}$ over $k \cap \mathfrak{P}$. Let π be an element of order one at $\mathfrak{P}$, and χ_π denote the map σ $(\in T) \mapsto \pi^{\sigma-1} \bmod \mathfrak{P}$. It is not difficult to show that $\mathrm{Hom}(T, (O_K/\mathfrak{P})^\times)$ is a cyclic group generated by χ_π and its order is e_0 ([Se]). Hence there is an integer n such that

$$z_\sigma \equiv \chi_\pi^{-n}(\sigma) \bmod \mathfrak{P}$$

for any $\sigma \in T$. Furthermore, we can show the following

PROPOSITION 2.1. *Let n be an integer satisfying*

$$z_\sigma \equiv \chi_\pi^{-n}(\sigma) \bmod \mathfrak{P}$$

for any $\sigma \in T$. Then

$$\mathrm{ord}_{\mathfrak{P}}\, g(z,\lambda) \equiv n \bmod e_0\,.$$

PROOF. Suppose $\mathrm{ord}_{\mathfrak{P}}\, g(z,\lambda) = m$. Then there is an element v in $K^\times$ prime to $\mathfrak{P}$ such that $g(z,\lambda) = \pi^m v$. For $\sigma \in T$, we have

$$g(z,\lambda)^{\sigma-1} = (\pi^{\sigma-1})^m v^{\sigma-1} \equiv \chi_\pi^m(\sigma) \bmod \mathfrak{P}\,.$$

Since $g(z,\lambda)^{\sigma} = z_{\sigma}^{-1} g(z,\lambda)$, we have $\chi_{\pi}^{m} \equiv \chi_{\pi}^{n}$. Hence $m \equiv n \bmod e_0$. □

For the rest of this section, we assume that p is an odd prime and splits completely in k. Moreover, we let $K = k(\zeta)$, where ζ is a primitive p-th root of unity. As is well-known, there is a unique element $\omega \in \mathrm{Hom}(\Gamma, (O_K/\mathfrak{P})^{\times})$ such that $\zeta^{\sigma} = \zeta^{\omega(\sigma)}$. Since ω is a generator of $\mathrm{Hom}(\Gamma, (O_K/\mathfrak{P})^{\times})$, there is an integer n such that

$$z_{\sigma} \equiv \omega^{-n}(\sigma) \bmod \mathfrak{P}$$

for $z \in Z^1(\Gamma, E_K)$. The next proposition is essentially due to Thaine ([T]).

PROPOSITION 2.2. *Let n be an integer satisfying*

$$z_{\sigma} \equiv \omega^{-n}(\sigma) \bmod \mathfrak{P}$$

for any $\sigma \in \Gamma$. Then

$$\mathrm{ord}_{\mathfrak{P}}\, g(z,\lambda) \equiv n \bmod p-1\,.$$

PROOF. Since p is unramified in k, $\mathrm{ord}_{\mathfrak{P}}(\zeta - 1) = 1$. Let m be an integer such that $\omega(\sigma) \equiv m \bmod \mathfrak{P}$. Then

$$\begin{aligned}\frac{(\zeta-1)^{\sigma}}{\zeta-1} = \frac{((\zeta-1)+1)^m - 1}{\zeta-1} &= \frac{1+\binom{m}{1}(\zeta-1)+\binom{m}{2}(\zeta-1)^2+\cdots-1}{\zeta-1}\\ &\equiv m \bmod \mathfrak{P} \equiv \omega(\sigma) \bmod \mathfrak{P}\,.\end{aligned}$$

Therefore, Proposition 2.2 is an easy consequence of Proposition 2.1. □

From Proposition 2.2 , we have the following decomposition

$$(g(z,\lambda)) = \mathfrak{A}(k)\prod_{\mathfrak{P}|p}\mathfrak{P}^{n(\mathfrak{P})}\,,$$

where for each prime of $\mathfrak{P}$ lying above p, $n(\mathfrak{P})$ is an integer satisfying $z_{\sigma} \equiv \omega^{-n(\mathfrak{P})}(\sigma) \bmod \mathfrak{P}$ and $\mathfrak{A}(k)$ is an ideal in k.

3. Cyclotomic units. Let m be a positive integer and ζ_m a primitive m-th root of unity. We assume that m is the conductor of $k = \boldsymbol{Q}(\zeta_m)$. Let p be a prime number and assume that m divides $p-1$. As in § 2, let ζ be a primitive p-th root of unity, $K = k(\zeta)$ and $\Gamma = \mathrm{Gal}(K/k)$. Let γ be a generator of Γ and let t be an integer with $t \not\equiv 0 \bmod m$. For a positive integer n we define an element z_{γ^n} as follows:

$$z_{\gamma^n} = (\zeta_m^t \zeta - 1)^{1+\gamma+\gamma^2+\cdots+\gamma^{n-1}}\,.$$

Since t is not divisible by m, z_{γ^n} is an element of E_K. Moreover,

$$\mathrm{N}_{K/k}(\zeta_m^t \zeta - 1) = \frac{\zeta_m^{tp} - 1}{\zeta_m^t - 1} = 1\,.$$

Hence, by Hilbert's Theorem 90, there is an element α of K such taht $\zeta_m^t \zeta - 1 = \alpha^{\gamma - 1}$. This implies that $z_{\gamma^n} = \alpha^{\gamma^n - 1}$. Therefore $z = \{z_{\sigma} \mid \sigma \in \Gamma\}$ is an element of $Z^1(\Gamma, E_K)$.

Let $\mathfrak{P}$ be a prime ideal of K over p, and let $\varepsilon(t) = \zeta_m^t - 1$. Then we have

$$z_{\gamma^n} \equiv \varepsilon(t)^n \bmod \mathfrak{P} .$$

As in §2, let ω be the element in $\mathrm{Hom}(\Gamma, (\boldsymbol{Z}/p)^\times)$ satisfying $\zeta^\rho = \zeta^{\omega(\rho)}$ for $\rho \in \Gamma$. Since $\mathfrak{P}$ is of absolute degree 1, for an element $\tau \in \mathrm{Gal}(K/\boldsymbol{Q})$ there is an integer s_τ such that

$$\varepsilon(t) \equiv \omega^{-s_\tau}(\gamma) \bmod \mathfrak{P}^\tau .$$

Let λ be an element of K satisfying $g(z, \lambda) \neq 0$. By Proposition 2.2, we have the following decomposition of principal ideal $(N_{K/k} g(z, \lambda))$:

$$(N_{K/k} g(z, \lambda)) = \mathfrak{A}(k)^{p-1} \prod_{\sigma \in G} \mathfrak{p}^{\sigma s_\sigma} ,$$

where $\mathfrak{A}(k)$ is an ideal in k, $\mathfrak{p} = \mathfrak{P} \cap k$ and $G = \mathrm{Gal}(k/\boldsymbol{Q})$. Let

$$\Theta(z, \varepsilon(t)) = \sum_{\sigma \in G} \sigma s_\sigma \in \boldsymbol{Z}[G] ,$$

where s_σ is an integer satisfying $\varepsilon(t) \equiv \omega^{-s_\sigma}(\gamma) \bmod \mathfrak{P}^\sigma$ for each $\sigma \in G$. Then we have the following

Proposition 3.1. *With the notation being as above, suppose that $p - 1$ is divided by the class number of k. Then $\mathfrak{p}^{\Theta(z, \varepsilon(t))}$ is a principal ideal.*

Let N be an integer and suppose that $N \equiv 0 \bmod mh$, where h is the class number of k. Let Δ be the subgroup of $k^\times$ generated by $\{1 - \zeta_m^a \mid 0 < a < m\}$. We let $D = \Delta E_k$ and, for brevity, write $\boldsymbol{Z}(N) = \boldsymbol{Z}/N\boldsymbol{Z}$. For an element $v \in \mathrm{Hom}(D, \boldsymbol{Z}(N))$ and $\varepsilon \in D$, we define

$$\eta(v, \varepsilon) = \sum_{\sigma \in G} v(\varepsilon^\sigma)\sigma^{-1} \in \boldsymbol{Z}(N)[G] .$$

Let l be a prime number such that $l \equiv 1 \bmod N$ and $\mathfrak{l}$ a prime ideal in k over l. Let $r = r(l)$ be a primitive root modulo l. Since $\mathfrak{l}$ is of absolute degree 1, there is an element $u_\mathfrak{l} = u(r, \mathfrak{l}) \in \mathrm{Hom}(D, \boldsymbol{Z}(N))$ such that $\delta^{(l-1)/N} \equiv r^{(l-1)u_\mathfrak{l}(\delta)/N} \bmod \mathfrak{l}$ for any element $\delta \in D$. Let r_0 be another primitive root modulo l and let $u_0 = u(r_0, \mathfrak{l})$. Then there is an integer s prime to $l - 1$ such that

$$r_0 \equiv r^s \bmod l .$$

Hence we have

$$\eta(u_\mathfrak{l}, \delta) = s\eta(u_0, \delta) .$$

By means of Proposition 3.1, we now prove

Proposition 3.2. $\eta(u_\mathfrak{l}, \zeta_m^t - 1) \in \boldsymbol{Z}(N)[G]$ *annihilates the ideal class of* $\mathfrak{l}$.

PROOF. Let γ_l be a generator of $\mathrm{Gal}(k(\zeta_l)/k)$ and, as above, $\omega_l \in \mathrm{Hom}(\mathrm{Gal}(k(\zeta_l)/k), (\boldsymbol{Z}/l)^{\times})$ satisfyng $\zeta_l^{\tau} = \zeta_l^{\omega_l(\tau)}$ for $\tau \in \mathrm{Gal}(k(\zeta_l)/k)$. By Proposition 3.1, $\sum_{\sigma \in G} \sigma s_\sigma$ annihilates the ideal class of $\mathfrak{l}$. Here, s_σ is an integer satisfying

$$\zeta_m^t - 1 \equiv \omega^{-s_\sigma}(\gamma_l) \bmod \mathfrak{l}^{\sigma} .$$

Let r_l be a primitive root modulo l such that $r_l \equiv \omega_l(\gamma_l) \bmod \mathfrak{l}$. Then

$$(\zeta_m^t - 1)^{(l-1)/N} \equiv r_l^{-(l-1)s_\sigma/N} \bmod \mathfrak{l}^{\sigma} .$$

Hence there is an integer s prime to $l-1$ such that

$$s_\sigma \equiv s u_{\mathfrak{l}}((\zeta_m^t - 1)^{\sigma^{-1}}) \bmod N .$$

Therefore, we have

$$\sum_{\sigma \in G} \sigma s_\sigma \equiv s\eta(u_{\mathfrak{l}}, \zeta_m^t - 1) \mod N ,$$

which proves Proposition 3.2.

Given an ideal class c of k, we define $P_N(c)$ as the set of prime ideals $\mathfrak{l}$ in c lying above rational primes $\equiv 1 \bmod N$. Let $k^+ = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ and $O_k^+ = k^+ \cap O_k$. For each element $\mathfrak{l}$ of $P_N(c)$ we select a primitive root $r = r(\mathfrak{l})$ modulo l $(l\boldsymbol{Z} = \mathfrak{l} \cap \boldsymbol{Z})$. Let $L_N(c)$ be the subgroup of $\mathrm{Hom}(D^+, \boldsymbol{Z}(N))$ generated by $\{u(r, \mathfrak{l})|_{D^+} \mid \mathfrak{l} \in P_N(c)\}$, where $D^+ = \{\alpha \in D \cap k^+ \mid \alpha > 0\}$. Then we have

PROPOSITION 3.3. *If φ is an element of* $\mathrm{Hom}(D^+, \boldsymbol{Z}(N))$, *then* $2\varphi \in L_N(c)$.

For the proof of this proposition, we need the following lemmas.

LEMMA 3.4. *$P_N(c)$ is an infinite set.*

PROOF. Let ζ_N be a primitive N-th root of unity and let $F = \boldsymbol{Q}(\zeta_N)$. We assume that N is the conductor of F. It is well-known that there are infinitely many prime ideals of absolute degree 1 in any ideal class of F, and a rational prime l splits completely in F if and only if $l \equiv 1 \bmod N$([L]). Let $N/m = \prod_{i=1}^{s} p_i^{e_i}$ be the prime factorization of N/m. Define $m_0 = m$ and $m_i = m_{i-1}p_i^{e_i}$ $(i = 1, \ldots, s)$. Let $F_i = \boldsymbol{Q}(\zeta_{m_i})$ and let C_i be the ideal class group in F_i. Since a prime ideal of F_i over p_i is totally ramified over F_{i-1}, the norm map $N_i : C_i \to C_{i-1}$ is surjective ([L2]). Therefore, there is an ideal class d in F such that $N_{F/k}(d) = c$. This implies that $P_N(c)$ is an infinite set. If N is not the conductor of F, we let $M = 2N$ and $F = \boldsymbol{Q}(\zeta_M)$. Since $P_M(c)$ is infinite and $P_M(c) \subset P_N(c)$, $P_N(c)$ is an infinite set. This proves Lemma 3.4.

The following lemma is due to Thaine ([T], Proposition 4 of §2).

LEMMA 3.5. *Let γ be a positive element of O_k^+. Suppose that for all, except possibly a finite set, prime ideals $\mathfrak{l} \in P_N(c)$ there exists $\beta_{\mathfrak{l}} \in O_k$ such that $\gamma \equiv \beta_{\mathfrak{l}}^N$* $\bmod \mathfrak{l}$. *Then $\gamma^2 = \beta^N$ for some $\beta \in O_k^+$.*

PROOF (Proof of Proposition 3.3). Let $V = D^+$. Since V/V^N is a finite abelian group, we have a dual paring

$$V/V^N \times \mathrm{Hom}(V, \boldsymbol{Z}(N)) \to \boldsymbol{Z}(N)\,.$$

If $L_N(c) \neq \mathrm{Hom}(V, \boldsymbol{Z}(N))$, then there is an element ε of $V - V^N$ such that $v(\varepsilon) = 0$ for any $v \in L_N(c)$. Let $u = u(r, \mathfrak{l}) \in L_N(c)$. Then

$$\varepsilon^{(l-1)/N} \equiv r^{(l-1)u(\varepsilon)/N} \equiv 1 \bmod \mathfrak{l}\,.$$

If s is an integer such that $\varepsilon \equiv r^s \bmod \mathfrak{l}$, then

$$\varepsilon^{(l-1)/N} \equiv r^{(l-1)s/N} \equiv 1 \bmod \mathfrak{l}\,.$$

Hence s is a multiple of N. By Lemma 3.5, $\varepsilon^2 = \beta^N$ for some $\beta \in O_k^+$. Since ε is an element of $D = \Delta E_k$, we have

$$\varepsilon = \varepsilon_0 \prod_{q|m} (\zeta_{q^i} - 1)^{a_q}\,,$$

where ε_0 is a unit of k, q ranges over the prime divisors of m and $i = i(q)$ denotes the maximum integer such that $q^i \mid m$. Let $\mathfrak{q}$ be a prime ideal above q in k. Then $2a_q = N\mathrm{ord}_{\mathfrak{q}}\beta \equiv 0 \bmod N$. Hence, if we write $b_q = \mathrm{ord}_{\mathfrak{q}}\beta$, then

$$\left(\frac{\beta}{\prod_l (\zeta_{q^i} - 1)^{b_q}}\right)^N = \varepsilon_0^2\,.$$

Therefore β is an element of D. If N is odd, then $\beta > 0$, otherwise $\varepsilon^2 = \beta^N = (-\beta)^N$. Hence we conclude that ε^2 is an element of V^N. By the duality we have $2\,\mathrm{Hom}(V, \boldsymbol{Z}(N)) \subset L_N(c)$. □

LEMMA 3.6. *Suppose that N is divisible by $4mh$. Let j be the complex conjugation, and let $\delta \in \Delta$ and $v \in \mathrm{Hom}(D,\ \boldsymbol{Z}(N))$. Then there is an element α in $\boldsymbol{Z}(N)[G]$ such that*

$$\eta(v,\ \delta^j) = \eta(v,\ \delta) + 2h\alpha\,.$$

PROOF. Since $(\zeta_m - 1)^j = -\zeta_m^{-1}(\zeta_m - 1)$, there is a root of unity ζ_0 in k such that $\delta^j = \delta\zeta_0$. Hence we have

$$\eta(v,\ \delta^j) = \eta(v,\ \delta) + \eta(v,\ \zeta_0)\,,$$

which implies that

$$\eta(v,\ \delta^j) - \eta(v,\ \delta) \in \frac{N}{2m}\boldsymbol{Z}(N)[G]\,,$$

because $2mv(\zeta_0) = 0$. By our assumption, we have $N/2m \equiv 0 \bmod 2h$. This completes the proof of Lemma 3.6.

Now, we can show the main theorem in this section. For any $u \in \mathrm{Hom}(D, \boldsymbol{Z})$ and $\varepsilon \in D$, we define

$$\theta(u, \varepsilon) = \sum_{\sigma \in G} u(\varepsilon^\sigma)\sigma^{-1} \in \boldsymbol{Z}[G]\,.$$

THEOREM 3.7. *Let u be an element of* $\mathrm{Hom}(D, \boldsymbol{Z})$. *Then for each $\delta \in \Delta$, $2\theta(u, \delta)$ annihilates the ideal class group of k.*

PROOF. We assume that N is divisible by $4mh$. For any $\varepsilon \in D$, we define $v \in \mathrm{Hom}(D, \boldsymbol{Z}(N))$ by $v(\varepsilon) \equiv u(\varepsilon) \bmod N$. Here we note $v(-\varepsilon) = v(\varepsilon)$. Let κ be an element in $\Delta \cap D_+$. Then

$$\eta(v, \kappa) = \sum_{\sigma \in G} v(\kappa^\sigma)\sigma^{-1} = \sum_{\kappa^\sigma > 0} v(\kappa^\sigma)\sigma^{-1} + \sum_{\kappa^\tau < 0} v(-\kappa^\tau)\tau^{-1} .$$

Let c be an ideal class. By Proposition 3.3, there are prime ideals $\mathfrak{l}_i$ $(i = 1, 2, \dots, s)$ in $P_N(c)$, $u_i = u(r_i, \mathfrak{l}_i) \in \mathrm{Hom}(D, \boldsymbol{Z}(N))$ and $a_i \in \boldsymbol{Z}(N)$ such that

$$2v(\gamma) = \sum_i a_i u_i(\gamma)$$

for any $\gamma \in D_+$. Hence we have

$$\begin{aligned} 2\eta(v, \kappa) &= \sum_{\kappa^\sigma > 0} \sum_i a_i u_i(\kappa^\sigma)\sigma^{-1} + \sum_{\kappa^\tau < 0} \sum_i a_i u_i(-\kappa^\tau)\tau^{-1} \\ &= \sum_{\sigma \in G} \sum_i a_i u_i(\kappa^\sigma)\sigma^{-1} + \sum_{\kappa^\tau < 0} \tau^{-1} \sum_i a_i u_i(-1) . \end{aligned}$$

Since $2u_i(-1) = u_i(1) = 0$, we have

$$2\eta(v, \kappa) = \sum_i \sum_{\sigma \in G} a_i u_i(\kappa^\sigma)\sigma^{-1} + \frac{N}{2}\alpha_0 ,$$

where $\alpha_0 \in \boldsymbol{Z}(N)[G]$.

Let t be an integer not divisible by m. Then

$$u((\zeta_m^t - 1)^j) = u(-\zeta_m^{-t}(\zeta_m^t - 1)) = u(\zeta_m^t - 1) ,$$

which implies that $v(\delta^j) = v(\delta)$ for any $\delta \in \Delta$. Hence, by Lemma 3.6, there is an element α in $\boldsymbol{Z}(N)[G]$ such that

$$\begin{aligned} 4\eta(v, \delta) = 2\eta(u, \delta^{1+j}) &= \sum_i a_i \eta(u_i,\ \delta^{1+j}) = \sum_i a_i \eta(u_i,\ \delta^2) + 2h\alpha \\ &= 2\sum_i a_i \eta(u_i,\ \delta) + 2h\alpha . \end{aligned}$$

Therefore, there exists an element $\beta \in \boldsymbol{Z}(N)[G]$ such that

$$2\eta(v,\ \delta) = \sum_i a_i \eta(u_i,\ \delta) + h\alpha + \frac{N}{2}\beta .$$

Hence, by Proposition 3.2, we conclude that $2\eta(v,\ \delta)$ annihilates c. This completes the proof of Theorem 3.7.

4. Class number formula. As in Section 3, we let $k = \boldsymbol{Q}(\zeta_m)$ and $G = \mathrm{Gal}(k/\boldsymbol{Q})$. For an element $c \in \boldsymbol{Z}(m)^\times$, we define $\sigma_c \in G$ by

$$\sigma_c : \zeta_m \mapsto \zeta_m^c .$$

Let $\hat{G} = \mathrm{Hom}(G, \boldsymbol{C}^\times)$ be the character group of G. For a character $\chi \in \hat{G}$, there is a unique primitive Dirichlet character χ_d such that $\chi(\sigma_c) = \chi_d(c)$. For $u \in \mathrm{Hom}(D, \boldsymbol{Z})$ and non-trivial character χ, we define $u(\chi)$ by

$$u(\chi) = \sum_{a=1}^{f-1} u(\zeta_f^a - 1)\chi_d(a) ,$$

where $f = f_\chi$ is the conductor of χ_d. We set $u(1) = 1$ for the unit character $1 = 1_\chi \in \hat{G}$. In the rest of this section, for a character $\psi \in \hat{G}$, we use the symbol ψ_d to denote the associated primitive Dirichlet character. Since $u(\zeta_f^{-a} - 1) = u(\zeta_f^a - 1)$, we have $u(\chi) = 0$ whenever χ_d is odd. Let $k^+ = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ and $G^+ = \mathrm{Gal}(k^+/\boldsymbol{Q})$. Let $\{\varepsilon_i\}$ be a free base of the unit group of k^+. We define

$$R_u = \det_{\tau \in G^+, i} (u(\varepsilon_i^\tau)) , \quad \tau \neq 1 .$$

Our aim in this section is to prove the following

THEOREM 4.1. *For an element $u \in \mathrm{Hom}(D, \boldsymbol{Z})$, we have*

$$h^+ R_u = \pm \prod_{\chi_d(-1)=1} \frac{1}{2} u(\chi) ,$$

where h^+ is the class number of k^+.

We prove first that there exists an element $u \in \mathrm{Hom}(D, \boldsymbol{Z})$ satisfying $R_u \neq 0$. For $\alpha \in D$ and $u \in \mathrm{Hom}(D, \boldsymbol{Z})$, we define $\theta_u(\alpha)$ by

$$\theta_u(\alpha) = \sum_{\sigma \in G} u(\alpha^\sigma)\sigma^{-1} .$$

Let T be a G-submodule of D, then the correspondence $\theta : u \mapsto \theta_u$ induces a map: $\mathrm{Hom}(T, \boldsymbol{Z}) \to \mathrm{Hom}(T, \boldsymbol{Z}[G])$. It is easy to see that θ is an injective homomorphism. Moreover, we have

LEMMA 4.2. $\mathrm{Im}\,\theta = \mathrm{Hom}_G(T, \boldsymbol{Z}[G])$.

PROOF. For $m \in T$ and $\phi \in \mathrm{Hom}(T, \boldsymbol{Z}[G])$, there are elements $\phi_\sigma \in \mathrm{Hom}(T, \boldsymbol{Z})$ such that

$$\phi(m) = \sum_{\sigma \in G} \phi_\sigma(m)\sigma^{-1} .$$

Hence, for an element $\rho \in G$, the equality $\rho\phi(m) = \phi(m^\rho)$ is equivalent to $\phi_{\rho\sigma}(m) = \phi_\sigma(m^\rho)$ for any $\sigma \in G$. Let e be the unit element of G. Then we have $\phi_\sigma(m) = \phi_e(m^\sigma)$. If we set $u = \phi_e$, then we have $\theta_u = \phi$. This implies that $\mathrm{Im}\,\theta \supset \mathrm{Hom}_G(T, \boldsymbol{Z}[G])$. It is easy to show the inverse inclusion. This completes the lemma.

LEMMA 4.3. *There is an element* $u \in \mathrm{Hom}(E, \boldsymbol{Z})$ *such that* $\mathrm{Ker}\, \theta_u = \mu_k$, *where* μ_k *is the group of roots of unity in* k.

PROOF. There is a unit η such that $E_\eta = \{\eta^\alpha \mid \alpha \in \boldsymbol{Z}[G]\}$ is a subgroup of finite index in E. Hence the homomorphism : $\alpha \mapsto \eta^\alpha$ induces the following homomorphism ϕ:

$$\boldsymbol{Q}[G] = \boldsymbol{Z}[G] \otimes \boldsymbol{Q} \xrightarrow{\phi} E \otimes \boldsymbol{Q} = E_\eta \otimes \boldsymbol{Q}\,.$$

Since $Q[G]$ is completely reducible by Maschke's theorem, there is a G-submodule M of $Q[G]$ such that $Q[G] = \mathrm{Ker}\,\phi \oplus M$. Moreover, the surjectivity of ϕ implies that M is isomorphic to $E \otimes \boldsymbol{Q}$. Hence there is an injective homomorphism:

$$E \otimes \boldsymbol{Q} \to \boldsymbol{Q}[G]\,,$$

which yields the sequence

$$E \to E \otimes \boldsymbol{Q} \to \boldsymbol{Q}[G]\,,$$

where the first arrow is the canonical homomorphism. Let f be the composition of the above homomorphisms. Then there is an integer t such that $tf(E) \subset \boldsymbol{Z}[G]$. It is obvious that the kernel of tf is μ_k. Hence, this lemma is derived from Lemma 4.2. □

LEMMA 4.4. *For an element* u *of* $\mathrm{Hom}(E, \boldsymbol{Z})$, *there is an element* v *of* $\mathrm{Hom}(D, \boldsymbol{Z})$ *such that* $v(\varepsilon) = u(\varepsilon)$ *for any* $\varepsilon \in E$.

PROOF. Since D/E is torsion-free, D/E is a free abelian group. Therefore, u can be extended on D. This completes the proof.

We define the subset $H \subset \mathrm{Hom}(D, \boldsymbol{Z})$ by

$$H = \{v \in \mathrm{Hom}(D, \boldsymbol{Z}) \mid v|_E = u \text{ and } \mathrm{Ker}\,\theta_u = \mu_k\}.$$

Then, by Lemmas 4.2 and 4.3, H is nonempty. Let $C = C_k = \Delta \cap E$ be the group of cyclotomic units, and let $v \in H$ and $u = v|_E$. Since $\mu_k \subset C$, θ_u induces the following isomorphism:

$$E/C \cong \theta_u(E)/\theta_u(C)\,.$$

Let s be the number of distinct primes dividing m. The group E/C is finite and the order is given by the following

THEOREM 4.5 (Sinnott [Si]). $[E : C] = 2^b h^+$. *Here* b *is an integer defined as follows*:

$$b = \begin{cases} 2^{s-2} - 1 - s\,, & s > 1\,, \\ 0\,, & s = 1\,. \end{cases}$$

Let $R = \boldsymbol{Z}[G]$ and $e_1 = 1/|G| \sum_{\sigma \in G} \sigma$. For any ideal $I \subset R$, we set $I_0 = \{\alpha \in I \mid e_1\alpha = 0\}$. Let $j = \sigma_{-1}$, and $J = \{1, j\} \subset G$. Let $\{\tau_i \mid i = 1, \dots, |G|/2\}$ be a complete set of representatives of G/J, and $\{\varepsilon_i\}$ a free base of E. We define $R_u(E)$ by

$$R_u(E) = \det_{i,j}\{u(\varepsilon_j^{\tau_i})\}\,, \quad i \neq |G|/2\,.$$

Since $u(N_{k/\boldsymbol{Q}}(\varepsilon)) = 0$ and $u(\varepsilon^{\sigma j}) = u(\varepsilon^{\sigma})$, it is easy to show $\theta_u(E) \subset (1+j)R_0$. Moreover, we have

LEMMA 4.6. *Let $u \in \mathrm{Hom}(E, \boldsymbol{Z})$. Then $R_u(E) \neq 0$ if and only if* $\mathrm{Ker}\,\theta_u = \mu_k$. *If $R_u \neq 0$, then $\theta_u(E)$ has finite index in $(1+j)R_0$ and the index is given by*

$$[(1+j)R_0 : \theta_u(E)] = |R_u(E)|\,.$$

PROOF. Since $\dim E \otimes \boldsymbol{Q} = \dim(1+j)R_0 \otimes \boldsymbol{Q}$, it is easy to show that $\theta_u(E)$ has finite index in $(1+j)R_0$ if and only if $\mathrm{Ker}\,\theta_u = \mu_k$. Let $T = \theta_u(E) + (1+j)\boldsymbol{Z}$. Since $(1+j)R_0 + (1+j)\boldsymbol{Z} = (1+j)R$, we have the following isomorphism

$$(1+j)R/T \cong (1+j)R_0/\theta_u(E)\,.$$

We select $\{(1+j)\tau_i^{-1}\}$ as a base of $(1+j)R$. Since $u(\varepsilon^{\sigma j}) = u(\varepsilon^{\sigma})$, we have

$$\theta_u(\varepsilon) = \sum_i u(\varepsilon^{\tau_i})(1+j)\tau_i^{-1}\,.$$

Hence we obtain that if $R_u(E) \neq 0$, then $[(1+j)R : T] = |R_u(E)|$. This proves the lemma.

In the rest of this section, we compute the index $[(1+j)R_0 : \theta_u(C)]$. The techniques here are due to Iwasawa and Sinnott [Si].

Let V be a finite dimensional $\boldsymbol{Q}$-vector space, and L, N finitely generated subgroup in V such that $L \otimes \boldsymbol{Q} = N \otimes \boldsymbol{Q} = V$. Then there is a nonsingular linear map $A : V \to V$ such that $A(L) = N$. We define

$$(L : N) = |\det(A)|\,.$$

Note that $(L : N)$ does not depend on the choice of A. We use the following properties. Let M be a finitely generated subgroup in V. If $(L : M)$, $(L : N)$ and $(M : N)$ are defined, then $(L : M)(M : N) = (L : N)$. If N is a subgroup of finite index in L, then $(L : N)$ is defined and $(L : N) = [L : N]$.

For a character $\chi \in \hat{G}$, we define the idempotent e_χ in $\boldsymbol{C}[G]$ by

$$e_\chi = \frac{1}{|G|}\sum_{\sigma \in G} \chi(\sigma)\sigma^{-1}\,.$$

Let f be a divisor of m . Then we define $H_f \subset G$ by

$$H_f = \{\sigma_t \in G \mid t \equiv 1 \bmod f, (t, m) = 1\}\,,$$

and let $s(H_f)$ denote the sum in $\boldsymbol{C}[G]$ of the elements of H_f. For a prime number p, let

$$\bar{\sigma}_p = \sum_\chi \bar{\chi}_d(p)e_\chi\,,$$

where $\bar{\chi}_d$ denotes the complex conjugate of the primitive Dirichlet character χ_d associated to $\chi \in \hat{G}$. For $v \in H$, let

$$\omega = \omega(v) = \sum_{\chi \neq 1} v(\bar{\chi})e_\chi\,,$$

the sum taken over the nontrivial characters χ of G. The following proposition is due to Sinnott [Si].

PROPOSITION 4.7.

$$(1-e_1)\theta_v(\Delta)=\omega\cdot U\,,$$

where e_1 is the idempotent associated to the trivial chatacter of G, and U is the R-module generated in $\boldsymbol{C}[G]$ by the elements of

$$\left\{s(H_f)\prod_{p|f}(1-\bar{\sigma}_p)\,\Big|\,f|m\right\}.$$

PROOF. For $r\in(1/m)\boldsymbol{Z}-\boldsymbol{Z}$, let

$$w(r)=v(e^{2\pi\sqrt{-1}r}-1)\,.$$

Then we have $w(r+1)=w(r)$. Let l be a divisor of m and satisfying $rl\notin\boldsymbol{Z}$. Then

$$\sum_{a=1}^{l}w\left(r+\frac{a}{l}\right)=w(lr)\,.$$

Hence, Proposition 4.7 follows from Sinnott's Proposition 2.1 ([Si]). □

COROLLARY 4.8. *Let* $u=v|_E\in\mathrm{Hom}(E,\,\boldsymbol{Z})$. *Then* $R_u=0$ *if and only if* $\prod_{\chi_d(-1)=1}v(\chi)=0$.

PROOF. For $\eta\in C$, we have

$$e_1\theta_v(\eta)=\frac{1}{|G|}\theta_v(\eta^{s(G)})=0\,.$$

Hence, $\theta_v(C)=(1-e_1)\theta_v(C)$ is a submodule of $(1-e_1)\theta_v(\Delta)$. Since

$$|G|(1-e_1)\theta_v(\Delta)\subset\theta_v(C)$$

and

$$(1-e_1)\theta_v(\Delta)\supset(1-e_1)\theta_v(C)=\theta_v(C)\,,$$

we have

$$\dim\theta_v(E)\otimes\boldsymbol{Q}=\dim(1-e_1)\theta_v(\Delta)\otimes\boldsymbol{Q}\,.$$

Therefore, by Proposition 4.7, we obtain $R_u=0$ if and only if $\dim\omega U\otimes\boldsymbol{Q}<|G|/2-1$. In order to prove this corollary, we may notice that

$$U\otimes\boldsymbol{Q}=\boldsymbol{Q}[G]$$

as stated in [Si, Proposition 2.2]. This proves the corollary.

If v is an element H, by Lemma 4.6, $[(1+j)R_0:\theta_v(E)]$ is finite. Hence, $[(1+j)R_0:\theta_v(C)]$ is also finite. Here we write, formally,

$$\begin{aligned}&[(1+j)R_0:\theta_v(C)]\\&\quad=((1+j)R_0:(1+j)U_0)((1+j)U_0:(1-e_1)\theta_v(\Delta))((1-e_1)\theta_v(\Delta):\theta_v(C))\,.\end{aligned}$$

The number $((1+j)R_0 : (1+j)U_0)$ does not depend on the choice of $v \in H$, and is computed by Sinnott. Moreover, the computation of$((1+j)U_0 : (1-e_1)\theta_v(\varDelta))$ is essencially the same as in [Si]. Hence we have

$$((1+j)U_0 : (1-e_1)\theta_v(\varDelta)) = ((1+j)U_0 : \omega U) = \left| \prod_{\chi(j)=1} \frac{1}{2} v(\chi) \right| ,$$

where the product is taken over the nontrivial characters χ of G satisfying $\chi(j) = 1$.

The following lemma completes our theorem.

LEMMA 4.9. *If s is the number of distinct primes dividing m, then*

$$[(1-e_1)\theta_v(\varDelta) : \theta_v(C)] = |G|2^{-s} .$$

PROOF. Let $m = \prod_{i=1}^{s} p_i^{e_i}$ be the primary decomposition of m and $\pi_i = \zeta_{p_i^{e_i}} - 1$. Since $\varDelta/C$ is a free abelian group generated by $\{\pi_i C\}$, we have

$$\theta_v(\varDelta) = \sum_{i=1}^{s} \boldsymbol{Z}\theta_v(\pi_i)\theta_v(C) .$$

Let T_i be the inertia group in G of a prime ideal over p_i. Then it is well-known that G is the internel direct product of T_i. Let $Z_i = \prod_{j \neq i} T_j$. Then we have $s(G) = s(Z_i)s(T_i)$ and $|G| = |Z_i||T_i|$. Hence,

$$e_1\theta_v(\pi_i) = \frac{s(Z_i)}{|Z_i||T_i|}\theta_v(\pi_i^{s(T_i)}) = \frac{1}{|T_i|}\theta_v(p_i) .$$

Let η be an element of $\varDelta$. Then we have

$$\theta_v(\eta) = \theta_v(\varepsilon) + \sum_i \alpha_i \theta_v(\pi_i) ,$$

where $\varepsilon \in C$ and $\alpha_i \in R$. Moreover, we write $\alpha_i = \sum_\sigma \alpha_i(\sigma)\sigma$ $(\alpha_i(\sigma) \in \boldsymbol{Z})$ and $\alpha_i(0) = \sum_\sigma \alpha_i(\sigma)$. Since

$$e_1\theta_v(\eta) = \sum_i e_1\alpha_i\theta_v(\pi_i) = \sum_i \alpha_i(0)\frac{1}{|T_i|}\theta_v(p_i) ,$$

we have

$$\begin{aligned}(1-e_1)\theta_v(\eta) &\equiv \sum_i \alpha_i(0)\left(\theta_v(\pi_i) - \frac{1}{|T_i|}\theta_v(p_i)\right) \bmod \theta_v(C) \\ &\equiv \sum_i \frac{\alpha_i(0)}{|T_i|}\theta_v\left(\frac{\pi_i^{|T_i|}}{p_i}\right) ,\end{aligned}$$

which implies that $(1-e_1)\theta_v(\varDelta)/\theta_v(C)$ is generated by

$$\left\{ \frac{1}{|T_i|}\theta_v\left(\frac{\pi_i^{|T_i|}}{p_i}\right)\theta_v(C) \right\} .$$

Suppose that there exist $\{r_i\} \subset \boldsymbol{Z}$ and $\delta \in C$ satisfying

$$\sum_{i=1}^{s} \frac{r_i}{|T_i|} \theta_v\left(\frac{\pi_i^{|T_i|}}{p_i}\right) = \theta_v(\delta) .$$

Let $u = v|_E$. We note that $\pi_i^{|T_i|}/p_i$ is a unit in k and, by our assumption, $\operatorname{Ker} \theta_u = \mu_k$. Hence there is an element ζ_0 of μ_k satisfying

$$\prod_i \left(\frac{\pi_i^{|T_i|}}{p_i}\right)^{r_i|Z_i|} = \zeta_0 \delta^{|G|} .$$

Let $p_i^{1/|T_i|}$ be the unique positive root of the following equation:

$$X^{|T_i|} = p_i .$$

Then there is a root of unity ξ satisfying

$$\prod_i \left(\frac{\pi_i}{p_i^{1/|T_i|}}\right)^{r_i} = \xi\delta .$$

Let

$$\beta = \prod_i p_i^{r_i/|T_i|} .$$

Since $\beta \in \boldsymbol{Q}(\zeta_m, \xi)$, $\boldsymbol{Q}(\beta)$ is a real abelian extension over $\boldsymbol{Q}$. Hence for any $\sigma \in \operatorname{Gal}(\boldsymbol{Q}^{\mathrm{ab}}/\boldsymbol{Q})$, $\beta^{\sigma-1}$ is real and a root of unity. Therefore we conclude that β^2 is an integer. This implies $r_i \equiv 0 \bmod |T_i|/2$ for all i.

On the other hand, we have

$$\frac{|T_i|}{2}(1-e_1)\theta_v(\pi_i) = \frac{1}{2}\theta_v\left(\frac{\pi_i^{|T_i|}}{p_i}\right) = \frac{1}{2}\theta_v(\pi_i^{|T_i|-s(T_i)}) = \frac{1}{2}\sum_{\sigma \in T_i} \theta_v(\pi_i^{1-\sigma}) .$$

We note that $\{\sigma|_{\boldsymbol{Q}(\pi_i)} \mid \sigma \in T_i\} = \operatorname{Gal}(\boldsymbol{Q}(\pi_i)/\boldsymbol{Q})$. Hence there is an element $\rho \in T_i$ such that $\rho = j|_{\boldsymbol{Q}(\pi_i)}$. Therefore, for $\sigma \in T_i$, we have

$$\pi_i^{\rho\sigma} = -\zeta_{p_i^{e_i}}^{-\sigma} \pi_i^{\sigma} ,$$

which implies that

$$\theta_v(\pi_i^{1-\rho\sigma}) = \theta_v(\pi_i^{1-\sigma}) .$$

Let $J_\rho = \{1, \ \rho\}$ and let $\{\tau_l\} \subset T_i$ be a representative of T_i/J_ρ. Then we obtain

$$\frac{1}{2}\sum_{\sigma \in T_i} \theta_v(\pi_i^{1-\sigma}) = \sum_l \theta_v(\pi_i^{1-\tau_l}) .$$

Hence,

$$\frac{|T_i|}{2}(1-e_1)\theta_v(\pi_i) \in \theta_v(C) .$$

We then conclude that

$$[(1-e_1)\theta_v(\varDelta) : \theta_v(C)] = \prod_i \frac{|T_i|}{2} = |G| \cdot 2^{-s} .$$

This completes the proof of Lemma 4.9.

Hence we have

$$[\theta_v(E) : \theta_v(C)] = \pm \frac{1}{|R_v(E)|}((1+j)R_0 : (1+j)U_0)|G|2^{-s} \prod_{\chi(j)=1, \chi\neq 1} \frac{1}{2} v(\chi) .$$

We now use the following formula:

THEOREM 4.10 (Sinnott [Si]).

$$[E : C] = h^+(e^+R_0 : e^+U_0)|G|Q2^{-s} ,$$

where $Q = [E : \mu_k E^+]$ *and* $e^+ = (1+j)/2$.

Consequently, we have

$$|R_v(E)|Qh^+ = \pm \prod_{\chi(j)=1, \chi\neq 1} \frac{1}{2} v(\chi) .$$

Let $\{\eta_i\}$ be a free base of E^+. As in §1, we define

$$R_v = \det_{i,j}\{v(\eta_j^{\tau_i})\},\ i \neq |G|/2 .$$

Then we have $R_v = \pm Q R_v(E)$. This proves Theorem 4.1.

5. The ideal of annihilators. Let $k = \boldsymbol{Q}(\zeta_m)$ and $G = \mathrm{Gal}(k/\boldsymbol{Q})$ as in §3. Let $j \in G$ be the complex conjugation and let $R = \boldsymbol{Z}[G]$. We assume that the conductor m is an odd prime power p^t. In this section we discuss the index $[R^+ : S]$, where $R^+ = (1+j)\boldsymbol{Z}[G]$ and S is the ideal of R generated by elements

$$\theta(u, \delta) = \sum_{\sigma\in G} u(\delta^\sigma)\sigma^{-1}$$

for all $\delta \in \varDelta$ and $u \in \mathrm{Hom}(D, \boldsymbol{Z})$. The fact that $S \subset R^+$ is easily derived from the following lemma.

LEMMA 5.1. $D^{1-j} = \varDelta^{1-j} = \mu$ *where* μ *is the group of roots of unity in* k.

PROOF. It is easy to show that $\varDelta^{1-j} = \mu$, and $E^{1-j} \subset \mu$. Hence $\mu = \varDelta^{1-j} \subset E^{1-j}\varDelta^{1-j} = \mu$. □

Since $\boldsymbol{Z}$ is torsion-free, $u(\zeta) = 0$ for any $u \in \mathrm{Hom}(D, \boldsymbol{Z})$ and $\zeta \in \mu$. By Lemma 5.1 we have

$$u(\delta^{\sigma j}) = u(\delta^\sigma) ,$$

which implies that $S \subset R^+$.

Let $\bar{D} = D/\mu$ and $\bar{\Delta} = \Delta/\mu$. Then $\bar{D}$ is a free abelian group. Let $k^+ = \boldsymbol{Q}(\zeta_m + \zeta_m^{-1})$ and $G^+ = \mathrm{Gal}(k^+/\boldsymbol{Q})$. It follows from Lemma 5.1 that j acts trivially on $\bar{D}$, and hence $\bar{\Delta}$ is a $\boldsymbol{Z}[G^+]$-module. Furthermore, we can prove the following lemma.

LEMMA 5.2. *$\bar{\Delta}$ is isomorphic to $\boldsymbol{Z}[G^+]$ as a $\boldsymbol{Z}[G^+]$-module.*

PROOF. We note that for any integer t prime to m, there is an element σ of G such that $(\zeta_m - 1)^\sigma = \zeta_m^t - 1$. Let G_{p^i} be the unique subgroup of G of order p^i $(i < r)$, and F the fixed field of G_{p^i} in k. Then we have

$$\prod_{\rho \in G_{p^i}} (\zeta_m - 1)^\rho = N_{k/F}(\zeta_m - 1) = \zeta_m^{p^i} - 1\,.$$

Therefore, for any element $\delta \in \Delta$, there is an element $\alpha \in R$ such that $\delta = (\zeta_m - 1)^\alpha$. Let ι be the canonical homomorphism $\iota : D \to \bar{D}$ and $\kappa = \iota(\zeta_m - 1)$. We define the homomorphism $\psi : \boldsymbol{Z}[G^+] \to \bar{\Delta}$ by $\psi(\alpha) = \kappa^\alpha$. Since $\bar{\Delta}$ is generated by κ as a $\boldsymbol{Z}[G^+]$-module, ψ is surjective. We note that $\Delta \cap E$ is the group of cyclotomic units in k. By the class number formula of cyclotomic fields, $\Delta \cap E$ is a subgroup of E of finite index. Hence Δ is also of finite index in D. Therefore, by Dirichlet's unit theorem, the rank of $\bar{\Delta}$ is equal to the order of G^+. This proves Lemma 5.2 .

For $v \in \mathrm{Hom}(\bar{D}, \boldsymbol{Z})$ and $\gamma \in \bar{\Delta}$, we define $\phi(v, \gamma) \in \boldsymbol{Z}[G^+]$ as follows:

$$\phi(v, \gamma) = \sum_{\sigma \in G^+} v(\gamma^\sigma)\sigma^{-1}\,.$$

Let $S(\bar{\Delta})$ denote the ideal of $\boldsymbol{Z}[G^+]$ generated by the elements $\phi(v, \gamma)$ with $\gamma \in \bar{\Delta}$ and $v \in \mathrm{Hom}(\bar{D}, \boldsymbol{Z})$. The following proposition is essential in this section.

PROPOSITION 5.3. $(\boldsymbol{Z}[G^+] : S(\bar{\Delta})) = (D : \Delta)$.

PROOF. Let $r = [k^+ : \boldsymbol{Q}]$. Since $\bar{D}$ is a free abelian group of rank r, $\mathrm{Hom}(\bar{D}, \boldsymbol{Z})$ is also a free abelian group of rank r. Let $\{u_i \mid i = 1, \dots, r\}$ be a base of $\mathrm{Hom}(\bar{D}, \boldsymbol{Z})$. We first prove that $S(\bar{\Delta})$ is generated by $\{\phi(u_i, \kappa)\}$ as an abelian group, where κ is the same as in the proof of Lemma 5.2. Let $u \in \mathrm{Hom}(\bar{D}, \boldsymbol{Z})$ and $\delta \in \bar{\Delta}$. Then there are integers a_i , b_σ such that $u = \sum_{i=1}^r a_i u_i$ and $\delta = \prod_{\sigma \in G^+} \kappa^{\sigma b_\sigma}$. Hence we have

$$\phi(u, \delta) = \sum_{i,\sigma} a_i b_\sigma \phi(u_i, \kappa^\sigma)\,.$$

For each $\sigma \in G^+$ and $u \in \mathrm{Hom}(\bar{D}, \boldsymbol{Z})$, we define u^σ as follows:

$$u^\sigma(\delta) = u(\delta^\sigma)\,.$$

It is clear that u^σ is an element of $\mathrm{Hom}(\bar{D}, \boldsymbol{Z})$. Hence, for each i and σ, there are integers $c_{ij}(\sigma)$ such that

$$\phi(u_i, \kappa^\sigma) = \phi(u_i^\sigma, \kappa) = \sum_j c_{ij}(\sigma)\phi(u_j, \kappa)\,.$$

This proves that $S(\bar{\varDelta})$ is generated by $\{\phi(u_i, \kappa)\}$. To prove Proposition 5.3 it suffices to show the following equality:

$$\det_{i,\sigma}(u_i(\kappa^\sigma)) = \pm(\bar{D} : \bar{\varDelta}) .$$

Since $\{\kappa^\sigma\}$ is a base of $\bar{\varDelta}$, it is easy to show that the absolute value of $\det\{u_i(\kappa^\sigma)\}$ is equal to $(\bar{D} : \bar{\varDelta})$. This proves the proposition.

THEOREM 5.4. *Let $R^+ = (1 + j)\boldsymbol{Z}[G]$ and S the ideal of $\boldsymbol{Z}[G]$ generated by $\{\theta(u, \delta) \mid u \in \mathrm{Hom}(D, \boldsymbol{Z}), \delta \in \varDelta\}$. Then $(R^+ : S) = h^+$, where h^+ is the class number of k^+.*

PROOF. The exact sequence $0 \to \mu \to D \to \bar{D} \to 0$ yields the following exact sequence:

$$\mathrm{Hom}(\bar{D}, \boldsymbol{Z}) \to \mathrm{Hom}(D, \boldsymbol{Z}) \to \mathrm{Hom}(\mu, \boldsymbol{Z}) = 0 .$$

Furthermore, $\mathrm{Hom}(\bar{D}, \boldsymbol{Z})$ and $\mathrm{Hom}(D, \boldsymbol{Z})$ have the same rank. Therefore $\mathrm{Hom}(D, \boldsymbol{Z})$ can be identified with $\mathrm{Hom}(\bar{D}, \boldsymbol{Z})$.

Let $J = \{1, j\} \subset G$. For each $\tau \in G$ the following map:

$$(1 + j)\tau \mapsto J\tau$$

induces an isomorphism

$$(1 + j)\boldsymbol{Z}[G] \to \boldsymbol{Z}[G/J] = \boldsymbol{Z}[G^+] .$$

For each coset $\tau \in G/J$ we let $\bar{\tau}$ be a coset representative. Then we have

$$\theta(u, \delta) = \sum_{\tau \in G^+} u(\delta^{\bar{\tau}})\bar{\tau}^{-1} + \sum_{\tau \in G^+} u(\delta^{\bar{\tau} j})\bar{\tau}^{-1} j = (1 + j) \sum_{\tau \in G^+} u(\delta^{\bar{\tau}})\bar{\tau}^{-1} ,$$

which implies that

$$\boldsymbol{Z}[G^+]/S(\bar{\varDelta}) \simeq R^+/S .$$

By Proposition 5.3 we have $(R^+ : S) = (\bar{D} : \bar{\varDelta})$. Since $\mu \subset \varDelta$ by Lemma 5.1, we have

$$(\bar{D} : \bar{\varDelta}) = (D : \varDelta) .$$

Hence we have

$$(R^+ : S) = (E\varDelta : \varDelta) = (E : E \cap \varDelta) .$$

We note that $E \cap \varDelta$ is the group of cyclotomic units. Theorem 5.4 is then immediate from the class number formula ([L2]). □

REFERENCES

[L] S. LANG, Algebraic number theory, Addison-Wesley, Reading, Mass., 1970.

[L2] S. LANG, Cyclotomic fields, Springer-Verlag, New York, 1978.

[Se] J. P. SERRE, Corps locaux, Publications de l'Institut de Mathématique de l'Université de Nancago VIII, Hermann, Paris, 1962.

[Si] W. SINNOTT, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math. (2) 108 (1978), 107–134.

[T] F. THAINE, On the ideal class groups of real abelian number fields, Ann. of Math. (2) 128 (1988), 1–18.

SHIZUOKA COLLEGE
UNIVERSITY OF SHIZUOKA PREFECTURE
2–2–1 OSHIKA, SHIZUOKA 422–8021
JAPAN

E-mail address: tateyama@bambi.t.u-shizuoka-ken.ac.jp